Національний технічний Університет України
“Київський політехнічний інститут імені Ігоря Сікорського”
Міністерство освіти і науки України
Національний технічний Університет України
“Київський політехнічний інститут імені Ігоря Сікорського”
Міністерство освіти і науки України

Кваліфікаційна наукова
праця на правах рукопису

Циганкова Оксана Валентинівна

УДК 004.9

ДИСЕРТАЦІЯ

Методи підвищення швидкодії асиметричних криптосистем з використанням еліптичних кривих у формі Едвардса

05.13.21 системи захисту інформації
Інформаційна безпека

Подається на здобуття наукового ступеня кандидата технічних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ О.В. Циганкова

Науковий керівник Бессалов Анатолій Володимирович, д.т.н., професор

Київ, 2021 р.

АНОТАЦІЯ

Циганкова О.В. Методи підвищення швидкодії асиметричних криптосистем з використанням еліптичних кривих у формі Едвардса. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук (доктора філософії) за спеціальністю 05.13.21 «Системи захисту інформації».

Підготовка здійснювалася у Національному технічному університеті України «Київський політехнічний інститут імені Ігоря Сікорського».

Захист відбудеться у спеціалізованій вченій раді Національного технічного університеті України «Київський політехнічний інститут імені Ігоря Сікорського». – Київ, 2021.

Роботу присвячено дослідженню криптографічних властивостей еліптичних кривих у формі Едвардса (ЕКФЕ) з подальшим використанням їх в алгоритмах асиметричних криптосистем з метою підвищення їх швидкодії. Основну увагу зосереджено на еліптичних кривих у формі Едвардса над полями з модулем p, де p – просте число.

Аналіз існуючих досліджень показав, що при опису властивостей ЕКФЕ виникають неточності через некоректність існуючої класифікації кривих, запропонованою Д.Берстейном та співавторами. Проте існуючі протиріччя в опису властивостей кривих Едвардса не дозволяють дослідити ЕКФЕ з метою знаходження найшвидших та простіших у програмуванні кривих для використання їх у криптосистемах.

У дисертаційній роботі досліджено ЕКФЕ методом перебору різних властивостей параметрів кривої з використанням апарату кінцевих полів та алгебраїчної геометрії, та запропоновано нову повну класифікацію кривих в узагальненій формі Едвардса. Розроблено опис властивостей кривих, що належать до трьох, за новою класифікацією, різних класів повних, скручених та квадратичних кривих, та обґрунтовано пропозиції щодо їх використання в асиметричних криптосистемах. Було встановлено, що криві, які належать до

класів повних та скручених ЕКФЕ, мають певні переваги та можуть бути рекомендовані для застосування в асиметричних криптосистемах ECC (Elliptic Curve Cryptosystems). Також було з'ясовано, що ЕКФЕ класу квадратичних кривих мають деякі недоліки та не рекомендовані для застосування в асиметричних криптосистемах.

На основі нової запропонованої класифікації, було отримано умови існування ЕКФЕ з мінімальним кофактором порядку кривої, що дозволило розрахувати кількість кривих, які можуть бути використані щодо пошуку криптостійких ЕКФЕ для застосування в асиметричних криптосистемах. У результаті аналізу властивостей ЕКФЕ було доведено, що над простим скінченним полем існує приблизно 3/8 від загальної кількості еліптичних кривих в узагальненій формі Едвардса, які мають порядок $4n$, де n – просте, які можуть бути використані для пошуку криптостійких кривих в асиметричних криптосистемах.

Проведено порівняльний аналіз кількості операцій при експоненціюванні точок на кривих Едвардса та кривих у формі Вейєрштрасса, методом розрахунку кількості операцій в полі при виконанні групових операцій додавання і подвоєння точок кривої, що дозволило одержати аналітичні оцінки швидкості експоненціювання точки на різних кривих. Отримані результати аналізу показали, що експоненціювання точки класів повних і скручених (за новою класифікацією) ЕКФЕ швидше в 1.6 рази ніж експоненціювання точки на кривих у формі Вейєрштрасса, які використовуються в стандартних криптоалгоритмах ЦП. Особливо ЕКФЕ виграють при трійковому представленні числа скалярного множника генератора криптосистеми (k) .

Розроблено новий метод визначення порядків випадкових точок ЕКФЕ на основі висновків з доведення трьох теорем, щодо властивостей точок та параметрів кривої, що дозволяє максимально спростити знаходження точки простого порядку, яку можна використовувати як генератор криптосистеми. Через тестування координати випадкової точки запропоновано новий алгоритм пошуку генератора криптосистеми, за допомогою якого генератор

криптосистеми знаходиться швидше ніж у стандартних алгоритмів у $32(\log n)$ разів (де n – порядок генератора групи точок еліптичної кривої).

За застосуванням нових алгоритмів пошуку генератора криптосистеми та методу зменшення обчислень розраховано загальносистемні параметри 25 скручених та 39 повних криптостійких ЕКФЕ в простих полях з довжиною модулів поля, рекомендованих стандартами FIPS-186-2-2000, FIPS–186–4-2013 та ISO/IECCD 15946, що дозволяє рекомендувати їх використання у криптоалгоритмах.

Також у роботі запропоновано новий більш простий і швидший за існуючі метод знаходження порядку ЕКФЕ і реконструкції всіх точок kP повної кривої форми Едвардса, який має практичне значення для використання при викладанні дисциплін, пов'язаних с еліптичною математикою.

Дисертація складається зі вступу, чотирьох розділів, висновків, списку використаних джерел, чотирьох додатків.

У вступі обґрунтовано актуальність теми дисертаційної роботи, сформульовано мету і задачі дослідження, наукову новизну та практичне значення отриманих результатів. Наведено дані про впровадження результатів роботи, її апробацію, публікації та особистий внесок здобувача.

У **першому розділі** виконано критичний аналіз сучасного стану сфери використання асиметричної криптографії, загальних проблем стандарту цифрового підпису. Виконано огляд існуючих досліджень провідних спеціалістів з криптографічного захисту інформації. Проаналізовано рекомендації щодо розгляду властивостей ЕКФЕ над простим полем. На основі аналізу сформульовано актуальність теми дисертаційного дослідження, обумовлену високою швидкістю обчислювальних операцій та спрощення програмування на еліптичних кривих у формі Едвардса.

Наведено огляд основних теоретичних відомостей властивостей ЕКФЕ, наведені висновки щодо використання кривих в оригінальній формі Едвардса в криптографічних додатках.

Здійснено трансформацію еліптичної кривої у формі Вейєрштрасса, яка використовується у стандартних криптоалгоритмах, та наведено умови ізоморфізму ЕКФЕ та Вейєрштрасса. Виведено алгоритм обчислення параметрів ЕКФЕ над простим полем, ізоморфних канонічним еліптичним кривим в формі Вейєрштрасса, придатних щодо криптографічних додатків. Отримана залежність між параметром ЕКФЕ і параметрами ізоморфної їй кривої в канонічній формі, що забезпечує перехід з однієї форми ізоморфної кривої в іншу.

Запропоновано опис детермінованого алгоритму вбудовування ключа в точку еліптичної кривої та її відновлення на основі алгоритму шифрування Ель-Гамаля, розглянуто певні питання у випадку використання запропонованого алгоритму інкапсуляції ключа. Представлено дослідження стійкості алгоритму вбудовування ключа. Визначено напрям подальших досліджень.

У **другому розділі** наведено загальні теоретичні властивості ЕКФЕ. Представлено універсальний модифікований закон додавання та подвоєння точок. На основі нової модифікації ЕКФЕ, введена арифметика для групових операцій з особливими точками цих кривих, надано аналіз точок малих порядків і формули, що пов'язують їх з іншими точками кривої. З застосуванням нової модифікації на базі аналізу параметрів кривої з використанням апарату кінцевих полів та алгебраїчної геометрії проведено теоретичне дослідження та аналіз ЕКФЕ над простими скінченними полями характеристики $p > 3$. Представлено нову повну класифікацію кривих в узагальненій формі Едвардса. Проведено дослідження та розроблено опис властивостей ЕКФЕ над простими полями, виявлено та описано переваги та недоліки цих кривих з метою застосування їх у ECC та інших криптоалгоритмах.

Проведено аналіз повних і скручених та квадратичних (за новою класифікацією) ЕКФЕ та обґрунтовано існування близько половини цих кривих які мають мінімальний кофактор порядку кривої 4.

Знайдено та доведено умови ізоморфізму ЕКФЕ і кривих у формі Вейєрштрасса, що дозволяє стверджувати, що ЕКФЕ мають аналогічні вимоги

до забезпечення безпеки у відношенні рішення проблеми дискретного логарифма (DLP). Доведено теорема щодо визначення точного числа повних кривих Едвардса, ізоморфних кривим у формі Вейєрштрасса з ненульовими параметрами a и b. Наведено доказ двох тверджень щодо визначення порядків точок з використанням властивостей взаємозв'язку сімейств точок. На підставі цього розроблено та проілюстровано на прикладі новий метод реконструкції точок kP скалярного добутку ЕКФЕ, який у порівнянні з класичним методом послідовного обчислення усіх точок, знижує трудомісткість обчислення у 8 разів та прискорює і спрощує програмування.

У другій частині **розділу 2** було проведено порівняльний аналіз складності експоненціювання точки на скрученій і повній кривій Едвардса у порівнянні з кривою у формі Вейєрштрасса з застосуванням аналітичних оцінок кількості операцій у полі у групових операціях додавання і подвоєння точок, які необхідно здійснити при експоненціювання точки на скрученій і на повній кривій Едвардса і кривій у формі Вейєрштрасса. За результатами порівняльного аналізу кількості операцій, які необхідно здійснити при експоненціювання точки в проективних координатах на скрученій і на повній ЕКФЕ і кривій у формі Вейєрштрасса було визначено, що експоненціювання точки на ЕКФЕ швидше, ніж на кривих у формі Вейєрштрасса, більш ніж у 1,5 рази. Особливо ЕКФЕ виграють при трійковому представленні числа скалярного множника генератора криптосистеми.

Перша частина **третього розділу** присвячена дослідженню властивостей кривих Едвардса над простими полями, що належать до класу повних кривих за новою класифікацією, та методам знаходження точок заданого порядку з метою практичного застосування їх в асиметричних криптосистемах. Проведено аналіз циклічних ЕКФЕ, який дозволив виявити низку нових властивостей повної ЕКФЕ над простим полем. Сформульовано та доведено 3 теореми про властивості точок повної ЕКФЕ. На підставі доведення цих теорем запропоновано новий метод знаходження точки максимального порядку, який використано у розробці нового методу знаходження базової точки повної ЕКФЕ.

Друга частина **третього розділу** присвячена дослідженню властивостей скручених кривих Едвардса. Виконано порівняльний аналіз деяких властивостей скручених кривих Едвардса з повними та виявлено, що скручені ЕКФЕ мають головну відмінність – нециклічну структуру групи точок 2-го порядку і наявність серед них двох особливих точок (з діленням на 0 y-координати), що робить їх застосування в деяких задачах еліптичної криптографії проблематичним.

Знайдено та обґрунтовано умови існування точок 2, 4 і 8 порядків, при виконанні яких скручені ЕКФЕ мають порядок $N_E = 4n$ та відсутність особливих точок у підгрупі точок простого порядку n, що відповідає вимогам щодо кривих, які можуть бути застосовані для побудови криптоалгоритмів. Крім того, у процесі досліджень було виявлено, що скручені ЕКФЕ при $N_E = 4n$ мають точки максимального порядку $2n$, що прискорює пошук точки простого порядку у 2 рази. Така специфічна особливість надала змогу створити новий детермінований алгоритм визначення генератора криптосистеми на скручених ЕКФЕ.

Вперше отримані необхідні і достатні умови подільності на 2 точок скрученої кривої Едвардса на підставі яких розроблено нові методи знаходження порядку точок скрученої кривої, з застосуванням яких розроблено нові алгоритми визначення генератора криптосистеми.

Зроблено аналіз кількості операцій у полі у групових операціях додавання і подвоєння точок повних та скручених ЕКФЕ при знаходженні точок простого порядку – генератора криптосистеми.. За результатами порівняльного аналізу оцінок групових операцій визначено, що у загальному випадку найменших обчислювальних витрат вимагають операції на повних ЕКФЕ. Особливо повні ЕКФЕ виграють при подвоєнні, яке обходиться без операції множення на параметр кривої.

Запропоновано метод досягнення мінімальної складності операцій, за наслідком використання якого з’явилася можливість зменшити складність додавання у групі точок через зневагу параметрами як малими числами.

З використанням запропонованих методів знаходження точок простого порядку розроблено три алгоритми пошуку генератора криптосистеми на повних та скручених ЕКФЕ

У **четвертому розділі** розраховано складності обчислень операції пошуку генератора криптосистеми у алгоритмах, створених на ЕКФЕ у порівнянні зі стандартним на кривих у формі Вейєрштрасса. Проведено порівняльний аналіз швидкості роботи алгоритмів на скрученій і повній ЕКФЕ у порівнянні з кривою у формі Вейєрштрасса. За аналізом складності операцій додавання і подвоєння точок на різних кривих визначено коефіцієнт виграшу у швидкості обчислень пошуку генератора на скрученої ЕКФЕ у порівнянні з стандартним алгоритмом, який приблизно $\approx O(\log n)$ разів менш, що стає максимальним виграшом у часової складової.

За використанням створених алгоритмів та розробленого методу зменшення складності операцій, розраховано загальносистемні параметри 25 криптостійких скручених та 39 повних ЕКФЕ над простим полем з довжиною модуля p = 192, 224, 256, 384 і 521 біт, які рекомендовані стандартами FIPS-186-2-2000, FIPS–186–4-2013 та ISO/IECCD 15946. Розраховані параметри крипостійких ЕКФЕ рекомендовані для практичного застосування у створенні нових криптостійких більш швидких, у порівнянні з стандартними, криптоалгоритмах ЦП. Результати розрахунків представлені у Додатку А.1 та Додатку А.2 дисертації.

Ключові слова: еліптична крива у формі Едвардса, параметри кривої, порядок точки, експоненціювання точок, повна крива Едвардса, скручена крива Едвардса, генератор криптосистеми, криптосистеми на еліптичних кривих, квадратичний лишок, квадратичний не лишок.

SUMMARY

Tsygankova O.V. Methods for increasing the speed of asymmetric cryptosystems using elliptic curves in Edwards form. – Manuscript.

The thesis for obtaining the Candidate of Technical Sciences degree of the specialty 05.13.21 – information security systems. – National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, 2021.

This work is dedicated to studying the cryptographic properties of elliptic curves in Edwards form (ECEF) and to the subsequent use of those in the asymmetric cryptosystem algorithms in order to increase their speed. The main focus is on the elliptic curves in the Edwards form over fields modulo p, where p is a prime.

Analysis of existing studies has shown that in describing the properties of ECEF, inaccuracies arise because of the incorrect classification of curves proposed by D. Bursten and co-authors. However, existing studies of the properties of the Edwards curves have not been sufficiently mathematically investigated to find the fastest and easiest to program curves for use in cryptosystems.

In this work, ECEF were investigated by means of a search of various properties of the curve parameters using the finite-field apparatus and algebraic geometry, which allowed creating a new complete classification of curves in the generalized Edwards form. A description of the properties of the curves belonging to the three, according to the new classification, of different classes of complete, twisted and quadratic curves was created, and proposals for their use in asymmetric cryptosystems were substantiated. Curves belonging to the classes of complete and twisted have been found to have certain advantages and may be recommended for use in the asymmetric cryptosystems ECC (Elliptic Curve Cryptosystems). Quadratic class curves have features and are not recommended for use in the asymmetric cryptosystems, but the possibility of using them in some cryptocurrencies is not excluded.

Based on the new proposed classification, conditions were obtained for the existence of ECEF with a minimum order coefficient of the curve, which allowed to calculate the number of curves that can be used to find crypto-resistant ECEF for use in the asymmetric cryptosystems. As a result of the calculations, it was obtained that

over a simple finite field there are about 3/8 of the total number of elliptic curves in the generalized Edwards form, which have order 4*n*, where *n* is a simple one, which can be used to find crypto-resistant curves for use in the asymmetric cryptosystems.

A comparative analysis of the exponential speed of points on the Edwards curves and the Weierstrass curves was performed, using the method of calculating the number of operations for the scalar product of the curve points, which allowed to obtain analytical estimates of the point exponential velocity on different curves. The results of the analysis show that the exponentiality of a point of classes of complete and twisted (by new classification) curves of Edwards is 1.6 times faster than the exponentiality of a point on the Weierstrass curves used in the crypto-algorithms of the CPU. In particular, the Edwards curves win with the triple representation of k.

A new method for determining the order of random points of the Edwards curve has been developed on the base of the conclusions of three theorems concerning the properties of points and curve parameters, which makes it possible to simplify the finding of a simple order point by testing the coordinate of a random point that can be used as a cryptosystem generator. A new algorithm for finding a cryptosystem generator using a new method of determining the order of the random points of the Edwards curve is proposed, which allows finding the cryptosystem generator on the Edwards curves $O(\log n)$ times (where *n* is the order of the generator of the group of points of the elliptic curve) faster than on the Weierstrass curves.

Using the new algorithms of cryptosystem generator search and the method of minimizing calculations, global system parameters for 25 twisted and 39 complete crypto-resistant elliptic curves in Edwards form over the simple fields with a modulo length recommended by standards FIPS-186-2-2000, FIPS–186–4-2013 and ISO/IECCD 15946, that allow to use them in cryptoalgorithms, are calculated.

In the work, a new, simpler and faster than the existing method of finding the ECFE order and reconstructions of all *kP* points of the complete Edwards curve, is proposed and can be used for teaching disciplines related to elliptical mathematics.

The dissertation consists of an introduction, four sections, conclusions, a list of sources used, five appendices.

The introduction substantiates the relevance of the topic of the dissertation, formulates the purpose and objectives of the research, scientific novelty and practical significance of the obtained results. The data on implementation of work results, its validation, publications and personal contribution of the applicant are given.

Section 1 provides a critical analysis of the current state of the art of using asymmetric cryptography, common problems of the digital signature standard. An overview of the existing research of leading experts in cryptographic information security has been completed. Recommendations for considering the properties of elliptic curves in the Edwards form over a simple field are analyzed. Based on the analysis, the relevance of the topic of the dissertation research is formulated, due to the high speed of computational operations and simplification of programming on elliptic curves in Edwards form.

The basic theoretical information about the properties of elliptic curves in Edwards form is given, the conclusions about the use of curves in the original Edwards form in cryptographic applications are given.

The transformation of the elliptic curve in the Weierstrass form used in standard crypto algorithms is performed, and the conditions of the Edwards curves and Weierstrass isomorphism are given. An algorithm for calculating the Edwards curves parameters over a simple field, isomorphic to the canonical elliptic curve in the Weierstrass form, suitable for cryptographic applications, is derived. The dependence between the Edwards curves parameter and the parameters of the isomorphic curve in a canonical form is obtained, which provides a simple transition from one form of the isomorphic curve to another.

The description of the algorithm of embedding the key in the point of the elliptic curve and its recovery on the basis of the ElGamal encryption algorithm is offered, the issues of using the proposed key encapsulation algorithm are considered. A study of the stability of the key embedding algorithm is presented. The direction of further research is determined.

Section 2 describes the general theoretical properties of elliptic curves in Edwards form. The universal modified law of adding and doubling points is presented.

Based on the new Edwards curves modification, the arithmetic for group operations with special points of these curves is introduced, the analysis of small order points and formulas that relate them to other points of the curve are given. Using a new modification based on the analysis of the parameters of the curve with the use of the finite-field apparatus and algebraic geometry, a theoretical study and analysis of the Edwards curves over simple finite fields of the characteristic p> 3 are researched. The new complete classification of curves in the generalized Edwards form is presented. A study was conducted and a description of the properties of the Edwards curves over simple fields was made, the advantages and disadvantages of these curves were identified and described in order to use them in ECC and other crypto algorithms.

The analysis of complete and twisted and quadratic (according to the new classification) Edwards curves is given, the existence of about half of these curves that have the minimum coefficient of the order of curve 4 is substantiated.

We find and prove the conditions of the curve of Edwardse isomorphism and the Weierstrass curves, which allows us to claim that the curve of Edwardse has similar security requirements for solving the discrete logarithm (DLP) problem. The theorem for determining the exact number of complete Edwards curves isomorphic to Weierstrass curves with nonzero parameters a and b is proved. The proof of two statements regarding the determination of the order of points and using the properties of the interconnection of the families of points is presented. On this basis, a new method of reconstruction of the points of the kP points of the scalar product of the curve of Edwardse was created and illustrated, which, in comparison with the classical method of sequential calculation of all points, reduces the complexity of calculation by 8 times and speeds up and simplifies programming.

In the second part of Section 2, a comparative analysis of the complexity of the exponentiality of a point on the complete and twisted Edwards curves compared to the Weierstrass curve using analytical estimates of the number of field operations in group operations of adding and doubling points to expose in exponentialization of a point on the twisted and complete Edwards curve and the Weierstrass curve, was performed.

According to the results of a comparative analysis of the number of operations to be performed when the exponentiality of a point in projective coordinates on the complete and twisted Edwards curves and the Weierstrass curve, it was determined that the exponentiality a point on the Edwards curves is faster than on the Weierstrass curve, more than 1.5 times. In particular, the Edwards curves win with the triple representation of number of the scalar multiplier of the cryptosystem generator.

The first part of Section 3 is devoted to the study of the properties of the Edwards curves over simple fields belonging to the class of complete curves according to the new classification, and methods of finding points of a given order for practical application of them in asymmetric cryptosystems. The analysis of cyclic curves in the form of Edwards, which revealed a number of new properties of complete Edwards curves over a simple field. Three theorems on the properties of points of complete Edwards curves are formulated and proved. Based on the proof of these theorems, a new method for determining the point of maximum order is proposed, which is used in the development of a new method for finding the base point of a complete Edwards curves.

The second part of Section 3 deals with the study of the properties of twisted Edwards curves. Comparative analysis of some properties of twisted Edwards curves with complete ones is performed, and it is revealed that the twisted Edwards curves have the main difference – noncyclic structure of group of points of 2nd order and presence among them of two special points (with division by 0 y-coordinates), which makes their application in some problems of elliptical cryptography are problematic.

The conditions of existence of points 2, 4 and 8 of orders in which the twisted Edwards curves are of order $N_E = 4n$ and the absence of singular points in the subset of points of prime order n are found and substantiated, which corresponds to the requirements for curves that can be applied for the construction of crypto algorithms. In addition, in the course of the research it was found that the twisted Edwards curves at $N_E = 4n$ have points of maximum order of $2n$, which accelerates the search for a point of simple order by 2 times. This specific feature made it possible to create a new

deterministic algorithm for determining the cryptosystem generator on the twisted Edwards curve.

For the first time necessary and sufficient conditions for splitting into two points of the twisted Edwards curves were obtained, which made it possible to propose new algorithms for determining the cryptosystem generator.

The analysis of the number of operations in the field in the group operations of adding and doubling points of complete and twisted Edwards curves when finding points of simple order – the cryptosystem generator, has done. According to the results of comparative analysis of estimates of group operations, it is determined that in the general case, the least costly operations require operations on complete curve of Edwards. Particularly complete Edwards curves win at doubling, which does without multiplying by a curve parameter.

We propose a method of achieving the minimum complexity of operations, as a result of which makes it possible to reduce the complexity of adding in a group of points due to neglect of parameters as small numbers.

Three algorithms for determining the cryptosystem generator on the complete and twisted Edwards curves are created by using the proposed methods of finding points of simple order.

Section 4 deals with calculations of the computing complexity of the operation of finding the cryptosystem generator in the algorithms created on the Edwards curves in comparison with the standard on the Weierstrass curve. A comparative analysis of the speed of the algorithms on the twisted and complete Edwards curves in comparison with the Weierstrass curve has done. According to the analysis of the complexity of addition and doubling points on different curves, the gain coefficient in the calculating speed of finding the generator on the twisted Edwards curve compared to the Weierstrass curve, which is approximately $\approx O(\log n)$ times less, which becomes the maximum gain in the time component, is defined.

Based on the created algorithms, the global system parameters of 25 crypto-resistant twisted and 39 complete Edwards curves over a simple field with a modulo length p = 192, 224, 256, 384 and 521 bits recommended by standards FIPS-186-2-

2000, FIPS–186–4-2013 and ISO/IECCD 15946, are presented. The calculated parameters of crypto-resistant Edwards curves are recommended for practical application in creation of new crypto-resistant faster, in comparison with standard, crypto-algorithms of the CPU. The results of the calculations are given in Appendix A.1 and Appendix A.2 of the dissertation.

Keywords: elliptic curves in Edwards form, curve parameters, point order, point exponentiation, complete Edwards curve, twisted Edwards curve, a cryptosystem generator, elliptic-curve cryptosystems, quadratic residue, quadratic non-residue.

Список публікацій здобувача за темою дисертації

1. Бессалов А.В., Цыганкова О.В. Взаимосвязь семейств точек больших порядков кривой Эдвардса над простым полем. Bessalov, A.V., Tsygankova, O.V. «Interrelation of families of points of high order on the Edwards curve over a primefield» // English translation of Problems of Informati on Transmission, 2015, Vol. 51, № 4, pp. 391-397. (проіндексовано в міжнародних наукометрічних базах РІНЦ, Scopus, Web of science).

2. Бессалов А.В., Цыганкова О.В. Число кривых в обобщенной форме Эдвардса с минимальным четным кофактором порядка кривой. // Проблемы передачи информации. Москва – Том 53, Вып. 1, март 2017, С. 101-111. *Transmission:* Bessalov A.V., Tsygankova O.V. «Number of curves in the generalized Edwards form with minima leven cofactor of the curve order» // English translation of Problems of Information 2017. (проіндексовано в міжнародних наукометрічних базах РІНЦ, Scopus, Web of science)

Статті в наукових журналах, що включені до переліку наукових фахових видань України

3. Бессалов А.В., Цыганкова О.В. Новые свойства эллиптической кривой в форме Эдвардса над простым полем. // Радиотехника №180, 2015. – С.137-143., Bessalov, A.V.,Tsygankova, O.V. «New properties of the Edwards form elliptic curveover a primefield» // Telecommunications and Radio Engineering (English

translation of Elektrosvyaz and Radiotekhnika) 2015. (проіндексовано в міжнародних наукометрічних базах Scopus та Web of science).

4. Бессалов А.В., Цыганкова О.В. Производительность групповых операций на скрученной кривой Эдвардса над простым полем. // Радиотехника №181, 2015.– С.58-63.

5. Бессалов А.В., Цыганкова О.В. Метод определения точек максимального порядка на кривой Эдвардса. // Спеціальні телекомунікаційні системи та захист інформації. Збірник наукових праць, випуск 2 (26), 2014. С.18-21.

6. Бессалов А.В., Цыганкова О.В. Классификация кривих в форме Эдвардса над простым полем. // Прикладная радиоэлектроника, 2015 Том 14 № 3, , С.197-203.

7. Бессалов А. В., Третьяков Д. Б., Цыганкова О. В. Свойства точек малих порядков кривых в обобщенной форме Эдвардса // Сучасний захист інформації № 2, 2016, С.46-54.

8. Циганкова О.В. Нові алгоритми знаходження базової точки на еліптичних кривих у формі Едвадса // «Інформаційні технології та комп'ютерна інженерія» № 1 (47) 2020. –С. 39-47.

Статті в інших наукових журналах

9. Bessalov A., Dykyi V., Malyshko A., Tsygankova O., Yadukha D. Parameters of the Fastest Cryptographically Strong Twisted Edwards Curves . // Theoretical and Applied Cybersecurity 2019. 1. c.7-11.

Тези доповідей в збірках матеріалів конференцій

1. Бессалов А.В., Цыганкова О.В. Свойства точек больших порядков кривой Эдвардса // тезиси докладів XVII міжнародної науково-практичної конференції «Безпека інформації в інформаційно-телекомунікаційних системах», Київ. – К.: НДЦ «Тезис», 2015 р. – С. 30-31.

2. Бессалов А.В., Цыганкова О.В. Классификация кривых в обобщенной форме Эдвардса. // тезиси докладів XVIII міжнародної науково-практичної

конференції «Безпека інформації в інформаційно-телекомунікаційних системах», Київ. – К.: НДЦ «Тезис», 2016 р. – С. 30-31.

3. Бессалов А.В., Олешко К.А., Поречна Д.Н., Циганкова О.В., Чорний О.Н. «Криптостійкі скручені ЕКФЕ з мінімальною складністю групових операцій» // тезиси докладів XIX міжнародної науково-практичної конференції «Безпека інформації в інформаційно-телекомунікаційних системах» Київ. – К.: НДЦ «Тезис», 2017 р. – С. 260.

4. Цыганкова О.В., Цыганков Р.И. Анимация точек экспоненцирования кривой Эдвардса // тезиси докладів XV Всеукраїнської наукова-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики», 25-27 травня 2017р., м. Київ. Том II.– С. 114.

5. Бессалов А.В., Циганкова О.В. Умови існування суперсінгулярних повних кривих Едвардса над простим полем // тезиси докладів XX Ювілейної міжнародної науково-практичної конференції «Безпека інформації у інформаційно-телекомунікаційних системах», Київ. – К.: НДЦ «Тезис», 2018 р., – С. 119-120.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ЦП – цифровий підпис.

ЕКФЕ - еліптичні криві у формі Едвардса.

NIST - National Institute of Standards and Technology Національний Інститут Стандартів і Технологій США.

ECC - Elliptic Curve Cryptosystems, криптосистеми на еліптичних кривих.

DSS - Digital Signature Standard, американський стандарт FIPS-186.

RSA - кріптографічній алгоритм з відкрітім ключем, що базується на обчислювальній складності задачі факторизації великих цілих чисел.

ECDSA - алгоритм з відкритім ключем для створення цифрового підпису, побудованій в групі точок еліптичної кривої (Elliptic Curve Digital Signature Algorithm).

ECKEP - протокол обчислення ключа еліптичної кривої (Elliptic Curve Key Establishment Protocol).

ВСТУП

Актуальність теми дослідження

Найважливішим завданням забезпечення інформаційної безпеки держави є створення та підтримання умов, що гарантують захист державних і особистих інформаційних ресурсів, безпечну обробку, зберігання та передачу інформації. Для захисту цих інформаційних ресурсів застосовується цифровий підпис (далі ЦП), який забезпечує процедуру автентифікації та отримується за результатом криптографічного перетворення набору електронних даних таємним ключем. Розвиток криптографічних методів, які використовуються для захисту державних та особистих інформаційних ресурсів, істотно впливає на інформаційну безпеку держави в цілому.

На сьогодні в Україні діють національні стандарти цифрового підпису ДСТУ 4145-2002 та ДСТУ ISO/IEC 14888-3:2014 в алгоритмах яких використовується криптографічні перетворення несуперсингулярних еліптичних кривих у формі Вейєрштрасса. В ДСТУ 4145-2002 використовуються криві у формі Вейєрштрасса над полями характеристики 2. Еліптичні криві, що використовуються в національному стандарті ЦП ДСТУ 4145, наразі відповідають сучасним вимогам безпеки, проте розвиток обчислювальної техніки призвів до постійного зростання об’єму та швидкості передачі інформації, яка потребує захисту і, як наслідок, до можливого зменшення терміну життя існуючих криптосистем. Оновлення існуючих або створення нових більш швидких криптосистем є актуальною задачею.

У 2015 році Koblitz N., Menezes A.J., в статті A Riddle Wrappedin an Enigma, (Technical Reports CACR-2015-14) зробили припущення щодо можливості використання властивостей еліптичних кривих у формі Едвардса (далі ЕКФЕ) в криптосистемах завдяки їх більш високої швидкості скалярного множення точок при експоненціюванні та меншої вразливості до атак з використанням інформації з побічного каналу. Також ці провідні вчені висловили сумніви щодо доцільності використання кривих Вейєрштрасса над полями характеристики 2, на яких часто

базуються алгоритми ЦП. Тому, для підвищення здатності діючих алгоритмів ЦП на кривих Вейєрштрасса задовольняти зростаючим вимогам щодо безпеки, виникає необхідність створення більш стійких та швидких алгоритмів ЦП на кривих у формі Едвардса. Це зумовлює актуальність дослідження властивостей еліптичних кривих у формі Едвардса над простими полями з метою застосування їх у сучасних, більш ефективних криптосистемах на еліптичних кривих.

Значний внесок у дослідженні властивостей ЕКФЕ, зробили: Koblitz N., Menezes A., EdwardsH., Washington L., BernsteinD., Lange T., Бессалов А.В., Ковальчук Л.В., Горбенко І.Д., Чевардін В.Є., Корнейко О.В. та інші. Разом з тим в цих наукових розробках не досліджувались ЕКФЕ з метою підвищення швидкодії асиметричних криптосистем, що і зумовило необхідність дослідити різні властивості криптостійких еліптичних кривих у формі Едвардса, придатних для використання в алгоритмах асиметричних криптосистем, зокрема, в алгоритмах цифрового підпису, які дозволять підвищити швидкість експоненціювання точки в цих криптосистемах.

Мета і завдання дисертаційного дослідження

Метою дисертаційного дослідження є підвищення швидкодії асиметричних криптосистем шляхом розроблення більш швидких за існуючі методів знаходження точок простого порядку та методів зниження складності експоненціювання точки з використанням властивостей еліптичних кривих у формі Едвардса.

Об'єктом дослідження є процеси перетворення інформації за допомогою асиметричних криптосистем, що базуються на складності задачі дискретного логарифмування на еліптичних кривих у формі Едвардса.

Предметом дослідження є властивості еліптичних кривих у формі Едвардса над простими полями та створені на їх основі алгоритми.

Наукове завдання дослідження

Створення методів підвищення швидкодії асиметричних криптосистем з використанням еліптичних кривих у формі Едвардса

Основні завдання дослідження

1. Проаналізувати властивості ЕКФЕ над простими полями з метою знаходження кривих, придатних для застосування у криптоалгоритмах.

2. Розробити методи зниження складності виконання операцій додавання та подвоєння точок ЕКФЕ.

3. Провести порівняльний аналіз складності експоненціювання точки кривих у формі Вейєрштрасса та ЕКФЕ.

4. Розробити методи підвищення швидкості знаходження точки простого порядку на ЕКФЕ над простими полями та провести порівняльний аналіз зі стандартними методами знаходження точки простого порядку.

5. Розробити більш швидкі за існуючі алгоритми пошуку генератора криптосистеми та розрахувати загальносистемні параметри кривих, придатних для застосування в асиметричних криптоалгоритмах.

Методи дослідження.

Проведені дослідження базуються на використанні основ алгебраїчної геометрії, абстрактної алгебри та теорії чисел (для дослідження властивостей ЕКФЕ, визначення кількісті кривих різних класів порядку $4n$, удосконаленню класифікації ЕКФЕ, розробці методів знаходження точки максимального порядку і базової точки, для оцінки виграшу алгоритмів пошуку генератора криптосистеми), теорії ймовірностей (для розробки методів оцінки швидкодії експоненціювання точки ЕКФЕ і методів її підвищення); теорії алгоритмів (для розробки алгоритмів знаходження точки простого порядку, та оцінки виграшу роботи алгоритмів).

Наукова новизна отриманих результатів визначається наступним:

1. Розроблено *нові* методи знаходження точки простого порядку на повних та скручених ЕКФЕ, на основі *нового* методу знаходження порядків випадкових

точок кривої Едвардса, які, за результатами порівняльного аналізу зі стандартними методами, швидше за існуючі.

2. *Вперше* дано оцінку кількості та визначено умови існування ЕКФЕ з корисними властивостями для криптосистем, які доцільно рекомендувати щодо створення асиметричних криптосистем.

3. *Вперше* дано оцінку складності експоненціювання точок на кривих у формі Едвардса, яка, у порівнянні з аналітичними оцінками складності експоненціювання точок кривих у формі Вейєрштрасса, значно менше, завдяки чому імплементація алгоритмів на кривих у формі Едвардса швидше за існуючі.

4. *Удосконалено* класифікацію кривих в узагальненій формі Едвардса, в якої, на відміну від існуючої, множину кривих розподіллено на три різних класи з різними за квадратичністю параметрами a і d, що надало можливість виявити класи кривих з корисними властивостями для застосування у криптоалгоритмах.

5. *Дістало подальшого розвитку* обчислення загальносистемних параметрів криптостійких скручених ЕКФЕ з урахуванням сучасних вимог щодо стійкості асиметричних криптосистем в рекомендованих стандартами FIPS-186-2-2000, FIPS–186–4-2013 та ISO/IECCD 15946 простих полях, які можуть бути рекомендовані для використання в алгоритмах асиметричних криптосистем.

Особистий внесок здобувача

Усі результати, що виносяться на захист, отримані автором особисто. У наукових працях, опублікованих у співавторстві, з питань, що стосуються даного дослідження, здобувачу належать: модифікація закону додавання точок на ЕКФЕ над простим полем, систематизація ознак кривих в узагальненій формі Едвардса, порівняльний аналіз кількості операцій при експоненціюванні точки на ЕКФЕ та на кривій у формі Вейєрштрасса, створення та описання нових алгоритмів знаходження базової точки на ЕКФЕ, порівняльний аналіз швидкодії створених алгоритмів пошуку генератора криптосистеми з швидкодією чинних алгоритмів стандарту ЦП, вибір параметрів a і d для розрахування загальносистемних параметрів 25 криптостійких скручених ЕКФЕ над простим скінченним полем,

розроблення методу реконструкції усіх точок ЕКФЕ, створення графічної ілюстрація скалярного добутку точок при експоненціюванні ЕКФЕ.

Здобувачу особисто належить

1. Модифікація закону складання точок на ЕКФЕ над простим полем [Бессалов А.В., Цыганкова О.В. Взаимосвязь семейств точек больших порядков кривой Эдвардса над простым полем. Bessalov, A.V., Tsygankova, O.V. «Interrelation of families of points of high order on the Edwards curve over a primefield» // English translation of Problems of Informati on Transmission, 2015, Vol. 51, № 4, pp. 391-397.];
2. Ідея побудови алгоритму знаходження точки простого порядку на ЕКФЕ [Бессалов А.В., Цыганкова О.В. Число кривых в обобщенной форме Эдвардса с минимальным четным кофактором порядка кривой. // Проблемы передачи информации. Москва – Том 53, Вып. 1, март 2017, С. 101-111.];
3. Застосування подвійної симетрії координат точок для аналізу їх властивостей [Бессалов А.В., Цыганкова О.В. Новые свойства эллиптической кривой в форме Эдвардса над простым полем. // Радиотехника №180, 2015. – С.137-143.,];
4. Оцінка складності операції подвоєння точок на ЕКФЕ над простим полем [Бессалов А.В., Цыганкова О.В. Производительность групповых операций на скрученной кривой Эдвардса над простым полем. // Радиотехника №181, 2015.– С.58-63.];
5. Пошук властивостей ЕКФЕ, що дозволяють знайти випадкову точку максимального порядку [Бессалов А.В., Цыганкова О.В. Метод определения точек максимального порядка на кривой Эдвардса. //Спеціальні телекомунікаційні системи та захист інформації. Збірник наукових праць, випуск 2 (26), 2014. С.18-21.];
6. Систематизація ознак класифікації кривих в узагальненій формі Едвардса. [Бессалов А.В., Цыганкова О.В. Классификация кривих в форме Эдвардса над простым полем. // Прикладная радиоэлектроника, 2015 Том 14 № 3, , С.197-203.], [Бессалов А.В., Цыганкова О.В. Классификация кривых в обобщенной форме Эдвардса. // тезиси докладів XVIII міжнародної науково-практичної конференції

«Безпека інформації в інформаційно-телекомунікаційних системах», Київ. – К.: НДЦ «Тезис», 2016 р. – С. 30-31.];

7. Аналіз особливих точок 2-го порядку ЕКФЕ [Бессалов А. В., Третьяков Д. Б., Цыганкова О. В. Свойства точек малих порядков кривых в обобщенной форме Эдвардса // Сучасний захист інформації № 2, 2016, С.46-54.];

8. Координація завдань виконавців та участь у розрахунку загальносистемних параметрів криптостійких скручених ЕКФЕ над простим скінченним полем [Bessalov A., Dykyi V., Malyshko A., Tsygankova O., Yadukha D. Parameters of the Fastest Cryptographically Strong Twisted Edwards Curves . // Theoretical and Applied Cybersecurity 2019. 1. c.7-11.];

9. Нові алгоритми пошуку генератора криптосистеми на ЕКФЕ над простим полем [Циганкова О.В. Нові алгоритми знаходження базової точки на еліптичних кривих у формі Едвардса // «Інформаційні технології та комп'ютерна інженерія» № 1 (47) 2020. –С. 39-47.];

10. Порівняльний аналіз швидкодії розроблених алгоритмів пошуку генератора криптосистеми з чинними алгоритмами стандарту ЦП [Бессалов А.В., Цыганкова О.В. Свойства точек больших порядков кривой Эдвардса // тезиси докладів XVII міжнародної науково-практичної конференції «Безпека інформації в інформаційно-телекомунікаційних системах», Київ. – К.: НДЦ «Тезис», 2015 р. – С. 30-31.];

11. *Систематизація ознак кривих в узагальненій формі Едвардса* [Бессалов А.В., Цыганкова О.В. Классификация кривых в обобщенной форме Эдвардса. // тезиси докладів XVIII міжнародної науково-практичної конференції «Безпека інформації в інформаційно-телекомунікаційних системах», Київ. – К.: НДЦ «Тезис», 2016 р. – С. 30-31.];

12. Постановка задачі та участь у роботі групи дослідників щодо розрахунку загальносистемних параметрів 25 криптостійких скручених ЕКФЕ над простим скінченним полем [Бессалов А.В., Олешко К.А., Поречна Д.Н., Циганкова О.В., Чорний О.Н. «Криптостійкі скручені ЕКФЕ з мінімальною складністю групових операцій» // тезиси докладів XIX міжнародної науково-практичної конференції

«Безпека інформації в інформаційно-телекомунікаційних системах» Київ. – К.: НДЦ «Тезис», 2017 р. – С. 260.];

13. Графічна ілюстрація скалярного добутку точок при експоненціюванні ЕКФЕ [Цыганкова О.В., Цыганков Р.И. Анимация точек экспоненцирования кривой Эдвардса // тезиси докладів XV Всеукраїнської наукова-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики», 25-27 травня 2017р., м. Київ. Том II.– С. 114.].

14. Участь в аналізі властивостей суперсінгулярних повних ЕКФЕ [Бессалов А.В., Циганкова О.В. Умови існування суперсінгулярних повних кривих Едвардса над простим полем // тезиси докладів XX Ювілейної міжнародної науково-практичної конференції «Безпека інформації у інформаційно-телекомунікаційних системах», Київ. – К.: НДЦ «Тезис», 2018, – С. 119-120.];

Апробація результатів дисертації. Низка положень дисертації доповідалися та обговорювалися на:

- Науковому семінарі «Проблеми сучасної криптології» (створеному за рішенням президії НАНУ у 2001 року), що проводиться в КПІ ім. Ігоря Сікорського;
- XVII Міжнародній науково-практичній конференції «Безпека інформації в інформаційно-телекомунікаційних системах» (26-28 травня 2015р., м. Київ);
- XVIII Міжнародній науково-практичній конференції «Безпека інформації в інформаційно-телекомунікаційних системах» (25-27 травня 2016р., м. Київ);
- XIX Міжнародній науково-практичній конференції «Безпека інформації в інформаційно-телекомунікаційних системах» (25-26 травня 2017р., м. Буча);
- XV Всеукраїнській наукова-практичній конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (25-27 травня 2017р., м. Київ);
- XX Міжнародній науково-практичній конференції «Безпека інформації в інформаційно-телекомунікаційних системах» (22-24 травня 2018р. м. Буча).

Структура та обсяг дисертації. Дисертація викладена на 145 сторінці, складається з вступу, чотирьох розділів, висновків, списку використаних джерел з 68 найменувань та 4 додатків. Загальний обсяг дисертації 145 сторінка, в тому числі 116 сторінок основного тексту та 7 сторінок використаних джерел. Робота містить 6 рисунків і 6 таблиць.

Зв'язок роботи з науковими програмами, планами, науково-дослідними роботами.

Робота виконувалася відповідно до планів наукових досліджень кафедри математичних методів захисту інформації Фізико-технічного інституту КПІ ім. Ігоря Сікорського в рамках наступних науково-дослідних робіт, виконаних на замовлення державних організацій:

1) «Дослідження та застосування сучасних математичних методів аналізу окремих перетворень у системах криптографічного захисту інформації» (шифр «Мокрель», номер держреєстрації 0115U004118);

2) «Дослідження методів криптоаналізу в застосуванні до сучасних систем криптографічного захисту інформації з урахуванням перспектив розвитку квантових обчислень» (шифр «Кобія», номер держреєстрації 0116U006384);

3) «Дослідження, розроблення і застосування методів криптоаналізу симетричних та асиметричних криптографічних систем» (шифр «Аргус», номер держреєстрації 0117U001817).

Дисертаційна робота також виконувалась в рамках науково-дослідних робіт на замовлення Міністерства освіти і науки України:

1) «Дослідження методів криптографічного аналізу систем захисту інформації в класичній та квантовій моделях обчислень з урахуванням додаткових даних та умов функціонування» № 2030-п (номер держреєстрації 0117U000500), з 01.01.2017 по 31.12.2019.

2) «Логіко-ймовірнісний підхід в задачах безпеки структурно-складних систем» № 2602-ф (номер держреєстрації 0113U002468), з 01.01.2013 по 31.12.2015.

Тематика роботи включена в науково-технічні плани кафедри математичних методів захисту інформації Фізико-технічного інституту КПІ ім. Ігоря Сікорського.

Практичне значення отриманих результатів полягає у наступному:

- запропоновано використання ЕКФЕ над простими полями в криптоалгоритмах для підвищення швидкодії асиметричних криптосистем;
- розроблено науково обґрунтовані нові методи генерування загальносистемних параметрів криптосистеми на основі арифметики ЕКФЕ, що зменшує кількість та складність групових операцій у сотні разів у порівнянні з алгоритмами, які використовуються у чинних стандартах ЦП;
- запропоновано новий метод пошуку генератора криптосистеми на скручених ЕКФЕ, який швидше стандартного у 32 ($\log n$) разів де n – порядок генератора;
- розраховано загальносистемні параметри 25 криптостійких скручених ЕКФЕ з урахуванням сучасних вимог щодо стійкості асиметричних криптосистем, які можуть бути рекомендовані для використання в сучасних асиметричних криптосистемах

Отримані результати було використано у наукових розробках на замовлення Служби зовнішньої розвідки України, а також впроваджено в навчальному процесі у викладанні навчальної дисципліни «Криптосистеми на еліптичних кривих» магістрам Фізико-технічного інституту КПІ ім. Ігоря Сікорського.

Результати дисертаційної роботи рекомендується використовувати при створенні алгоритмів асиметричних криптосистем.

РОЗДІЛ 1 СУЧАСНИЙ СТАН ЕЛІПТИЧНОЇ КРИПТОГРАФІЇ ТА ЗАДАЧІ ДОСЛІДЖЕНЬ

В даному розділі розглядаються сучасні зміни у сфері використання асиметричної криптографії, загальні проблеми національного стандарту цифрового підпису, а також наводяться необхідні теоретичні відомості з властивостей кривих у формі Едвардса (ЕКФЕ).

1.1 Аналіз існуючих форм еліптичних кривих і задачі досліджень

Вперше нову форму еліптичних кривих представив у своїй роботі професор математики Університету Нью-Йорка Гарольд Едвардс [1]. Вивчаючи праці Ейлера, Гауса та Абеля двохсотлітньої давності, він виявив рівняння, яке за допомогою раціональних перетворень приводиться до рівняння канонічної еліптичної кривої в формі Вейєрштрасса. Едвардсу вдалося знайти закон складання точок для цієї кривої і довести її ізоморфізм з кривою Вейєрштрасса. Ці два результату дали вченим вагомі підстави називати запропоновану форму рівняння кривими в формі Едвардса. Незабаром виявилося, що новий клас кривих має низку чудових властивостей. Ці властивості відразу були помічені і досліджені криптографами. Першою дуже конструктивною роботою в розвиток цього напрямку слід відзначити статтю Даніеля Бернстейна і Тані Ланге [2] (за нею пішла серія робіт цих та інших авторів). Автори [2] проаналізували властивості ЕКФЕ над кінцевим полем характеристики, не рівної 2. Вони модифікували оригінальну криву Едвардса, ввели новий параметр кривої d як квадратичний не лишок поля і отримали закон складання точок для модифікованої кривої. Ця модифікація дозволила перейти від нециклічного оригінальної ЕКФЕ з особливими точками до циклічної кривої без особливих точок. Також вони підкреслили важливу перевагу ЕКФЕ – це наявність одного параметра d замість двох для кривої Вейєрштрасса. Далі автори [2] довели, що поряд з властивостями повноти і універсальності закону складання, ЕКФЕ, серед відомих, [1] являються найпродуктивнішим тому, що в проективних координатах операції в групі додавання і подвоєння точок виконуються

мінімальною кількістю операцій в полі завдяки заміни точки на нескінченності афінної точкою (нейтральним елементом групи точок).

Унікальність ЕКФЕ полягає, насамперед, у тому, що всі її точки, включаючи нейтральний елемент групи, не є особливими. Це відразу знімає проблему, яка виникає при програмуванні операцій, що включають особливу точку з нескінченними координатами, яка характерна для всіх традиційних кривих в формі Вейєрштрасса. Така властивість ЕКФЕ прискорює програмну реалізацію і виконання криптоалгоритмів.

Найбільший внесок в розвиток теорії кривих Едвардса, в інтересах криптографії, американський вчений Даніель Бернстейн зі своїми співавторами. Поряд з вищесказаним про статтю [2] в його наступних роботах вперше визначено і досліджено властивості скручених ЕКФЕ [3], бінарних ЕКФЕ [4,5], запропонована арифметика проективних інвертованих координат для повних ЕКФЕ [6] з найменшою складністю групових операції складання точок. Такі властивості ЕКФЕ, безсумнівно, потребують дослідження з метою їх використання в криптоалгоритмах.

1.2 Аналіз сучасного стану стандартизації цифрового підпису в Україні

В Україні діє національний стандарт цифрового підпису ДСТУ 4145-2002 з арифметикою несуперсингулярних еліптичних кривих над розширеннями полів характеристики 2. За рекомендацією світових спеціалістів стандарти потребують оновлення кожні 4-5 років. З 2002 року національний стандарт не оновлювався.

Останнім часом в галузі криптографічного захисту інформації відбулися значні зміни, а саме:

- в усьому світі з'явилась значна кількість нових стандартів у сфері криптографічного захисту інформації і багато стандартів було замінено на більш сучасні, швидкі і криптографічно стійкі;
- з'явились нові алгебраїчні об'єкти, використання яких для побудови різних криптосистем мають численні переваги як у швидкодії, так і в криптографічній стійкості;

- з'явились нові криптографічні алгоритми ЕСС, які мають численні переваги перед старими і поступово їх витісняють;
- з'явились нові алгоритми криптоаналізу, внаслідок чого виникла необхідність переглянути чинні криптографічні алгоритми і, можливо, змінити деякі їх параметри;
- з'явилися пропозиції відомих експертів щодо використання в криптосистемах набагато більш ефективних кривих, ніж криві Вейєрштрасса над полями характеристики 2, що використовуються у протоколах цифрового підпису. Зокрема, існують рекомендації застосовувати еліптичні криві у формі Едвардса (ЕКФЕ) з найбільшою швидкодією та більш стійкими до атак побічного каналу;
- крім ЦП, асиметрична криптографія вирішує не менш важливе завдання - розподіл ключів (ECKEP) для симетричного шифрування. Протоколи ECKEP разом з алгоритмами ЦП входять в більшість міжнародних стандартів. Але їх немає в українських стандартах.

В Україні з 2002 року діє національний стандарт цифрового підпису ДСТУ 4145-2002 [10] з арифметикою несуперсингулярних еліптичних кривих над розширеннями полів характеристики 2. Крім того, в 2014 році в якості національного затверджений міжнародний стандарт ISO / IEC 14888-1,2,3: 2008 [11, 12, 13]. За оцінками великого числа експертів, криві над полями характеристики 2 мають чимало вразливих місць і їх слід уникати в криптосистемах [7]. Другий стандарт ISO / IEC також не містить рекомендацій щодо нових кривих.

У зв'язку з тим, що ДСТУ 4145-2002 має невисоку конкурентоздатність, його використання в країні - менше 10% в порівнянні зі стандартами, що включають RSA і ECDSA.

Проведено атаки та зламані ЕС над полями характеристики 2 з різною довжиною модуля. В 2002 році - 108 bit; в 2009 році - 111 bit; та в 2015 році - 113 bit.

Можна зробити висновки, що національні українські стандарти сильно застаріли і потребують оновлення.

З 2007 року провідні фахівці з криптології у своїх роботах неодноразово підкреслюють переваги та достоїнства ЕКФЕ. У своїй роботі Koblitz N., Menezes A.J. «A Riddle Wrapped in an Enigma, Technical Reports CACR-2015-14. 2015: Available: www.cacr.math.uwaterloo.ca.» [7] заявляють:

- «... ЕКФЕ мають найбільш швидке експоненціювання точки і кращий захист від можливих нападів з боку каналу і їх краще використовувати в криптоалгоритмах цифрового підпису ...»
- «… Слід зазначити, що в разі еліптичних кривих над простим полем, починаючи з 1997 року не були виявлені нові класи слабких еліптичних кривих. Зокрема не було виявлено недоліків в NIST кривих після того, як вони були запропоновані близько 18 років тому… »
- «.... в рішенні ECDLP на випадкової кривої над простим полем протягом всієї 30-річної історії ECC немає ніякого істотного прогресу, в той же час були великі прориви в проблемі факторизації цілого числа… »
- «… Через недавнього прогресу в атаці на ECDLP на кривих над двійковим полем за допомогою алгоритмів підсумовування поліномів, які були натхненні ідеєю I. Semaev [8] (див. [9]) деякі дослідники висловили сумніви щодо довгострокової безпеки всіх еліптичних кривих над двійковим полем, і ми вважаємо, що найбільш консервативним є вибір NIST кривих, визначених над простим полем. Ці криві позначені P-k, де k-bitlength. »

Також о перевагах ЕКФЕ йдеться в інших публікаціях світових фахівців [32 - 43]

На підставі попередніх досліджень, вочевидь, виникає необхідність в дослідженні нових властивостей еліптичних кривих в формі Едвардса для застосування їх в криптосистемах.

1.3 Еліптичні криві в оригінальній формі Едвардса

В роботі Гарольда Едвардса [1] розглядалися властивості еліптичної кривої в формі

$$x^2 + y^2 = e^2(1 + x^2y^2), \qquad (1.1)$$

до якої ще близько 2-х століть назад зустрічалася в роботах Ейлера і Гауса (при $e = 1$ і заміні знаку «+» на «−» у правій частині). Ці математики ще не знали, що рівняння (1.1) можна назвати еліптичної кривої, так як поняття це сформувалося майже через століття після введення закону складання точок кривої з утворенням структури абелевої групи точок. Едвардсу вперше вдалося довести, що рівняння (1.1) описує криву, ізоморфну кривій в формі Вейєрштрасса, і отримати закон складання її точок

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2+x_2y_1}{e(1+x_1x_2y_1y_2)}, \frac{y_1y_2 - x_1x_2}{e(1-x_1x_2y_1y_2)}\right) \quad (1.2)$$

Криві (1.1), в зв'язку з цим, називають *оригінальною формою Едвардса*. Нейтральним елементом тут є точка $O = (0, e)$, а зворотня точка визначена як $-(x_1, y_1) = (-x_1, y_1)$. З (1.2) випливає, що $(x_1, y_1) + (0, e) = (x_1, y_1)$ та $(x_1, y_1) + (-x_1, y_1) = (0, e)$.

Криві (1.1) існують над усіма полями з нульовою характеристикою і над кінцевими полями $F_p, 2D_0 = 0$. При збігу доданків точок універсального закону (1.2) отримуємо, в окремому випадку, закон подвоєння

$$2(x_1, y_1) = \left(\frac{2x_1y_1}{e(1+x_1^2y_1^2)}, \frac{y_1^2-x_1^2}{e(1-x_1^2y_1^2)}\right). \quad (1.3)$$

Підставляючи в праву частину точку $O = (0, e)$, отримаємо рішення для точки 2-го порядку $D_0 = (0, -e)$.

Для задач криптографії можуть виявитися цікаві лише криві виду (1.1) над полем F_q кінцевого порядку $q = p^m$. Заміною $x \to \frac{x}{e}$ крива (1.1) записується в ізоморфній формі

$$x^2 + y^2 = 1 + e^4x^2y^2 \Longrightarrow y^2 = \frac{1-x^2}{1-e^4x^2}, \; e^4 \neq 1. \quad (1.4)$$

При $e = 1$ при усіх значеннях x маємо 2 рішення $y = \pm 1$ і порядок такої кривої виходить за межі Хассе [15] - крива не є еліптичної. Крім того, виникають особливі випадки в законі подвоєння. Наприклад, подвоєння точки $P = (1,1)$, розв'язує рівняння (1.1), породжує невизначеність 0/0 для y - координати в (1.3). Слід тому прийняти $e^4 \neq 1$, тоді число рішень рівняння (1.4) обмежується числом елементів e^4 поля, що породжують квадрати в правій частині рівняння.

Для точки F_0 4-го порядку кривої (1.1), приймаючи $2F_0 = D_0$, отримуємо згідно (1.3)

$$\frac{2x_1y_1}{e(1+x_1^2y_1^2)} = 0, \quad \frac{y_1^2 - x_1^2}{e(1-x_1^2y_1^2)} = -e.$$

Звідки $y_1^2 = 0 \implies x_1^2 = e^2 \implies x_1 = \pm e$. Отже, для кривої (1.1) при $e^4 \neq 1$ над кінцевим полем характеристики $p \neq 2,3$, завжди існують 2 точки 4-го порядку $\pm F_0 = (\pm e, 0)$. Знайденими вище не обмежуються усі точки 2-го і 4-го порядків. Зокрема, завжди є ще дві особливі точки 2-го порядку (на нескінченності), і крива (1.1) є нециклічні (з трьома точками 2-го порядку).

З рівняння кривої (1.1) справедливі вирази для квадратів координат

$$y^2 = \frac{e^2 - x^2}{1 - e^2x^2}, \qquad x^2 = \frac{e^2 - y^2}{1 - e^2y^2}.$$

При нульових значеннях знаменників цих рівностей отримуємо 4 особливі точки кривої: $F_{1,2} = (\pm e^{-1}, \infty)$, $D_{1,2} = (\infty, \pm e^{-1})$. Знаком "∞" позначено ділення на 0. Хоча в кінцевому полі елементи не визначені, але в операціях в групі (1.2) і (1.3), що мають вигляд раціональних функцій, обидві координати точок входять в чисельник і знаменник. Це дозволяє користуватися формулами (1.2) і (1.3) в особливих точках, приймаючи правила звичайного граничного переходу. Тоді за допомогою (1.3) отримаємо

$2D_{1,2} = 2(\infty, \pm e^{-1}) = \left(0, \frac{\infty^2}{ee^{-2}\infty^2}\right)$=(0,e)=0.

$2F_{1,2} = 2(\pm e^{-1}, \infty) = \left(0, \frac{\infty^2}{-ee^{-2}\infty^2}\right) = (0, -e) = D_0.$

Звідси випливає, що особливі точки $D_{1,2}$ мають порядок 2, а особливі точки $F_{1,2}$ – порядок 4. Оригінальні ЕКФЕ, таким чином, мають властивості нециклічних кривих.

Аналогічно, для точки S 8-го порядку з урахуванням рівності $2S = F$ маємо

$$\frac{2x_1y_1}{e(1+x_1^2y_1^2)} = e, \quad \frac{y_1^2 - x_1^2}{e(1-x_1^2y_1^2)} = 0.$$

Тоді с урахуванням (1.1)

$$y_1^2 = x_1^2 \Longrightarrow x_1^4 - 2e^{-2}x_1^2 + 1 = 0 \Longrightarrow x_1^2 = e^{-2}\left(1 \pm \sqrt{1 - e^{-4}}\right).$$

При таких умовах точки 8-го порядку існують лише в разі, коли вираз в дужках існує і є квадратом. Наявність точок 8-го порядку лише збільшує значення кофактора порядку кривої до 16, 32 і т.д. Крім того, серед точок 2-го і 4-го порядків кривої (1.1) є особливі точки (на нескінченності), для яких слід вводити арифметику складання точок. Зазначені недоліки кривих в оригінальній формі Едвардса роблять їх практично нецікавими для криптографічних додатків.

1.4 ЕКФЕ з модифікацією Бернстейна-Ланге

Незабаром, після роботи [1] з'явилася значна робота фахівців з криптографії Даніеля Бернстейна і Тані Ланге [2], в якій запропонована модифікація кривої (1.1) з введенням параметру d - нелишок над кінцевим полем F_p^m характеристики $p \neq 2$ виду

$$E: x^2 + y^2 = e^2(1 + x^2y^2),\ d(1 - de^4) \neq 0,\ \left(\frac{d}{p}\right) = -1, \tag{1.5}$$

Де $\left(\frac{d}{p}\right) -$ символ Лежандра та параметр $d -$ квадратичний нелишок [15,21]. Універсальний закон складання для точок цієї кривої має вигляд

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + x_2y_1}{e(1 + x_1x_2y_1y_2)},\ \frac{y_1y_2 - x_1x_2}{e(1 - x_1x_2y_1y_2)}\right) \tag{1.6}$$

Закон подвоєння для співпадаючих точок, відповідно, записується як

$$2(x_1, y_1) = \left(\frac{2x_1y_1}{e(1 + dx_1^2y_1^2)},\quad \frac{y_1^2 - x_1^2}{e(1 - dx_1^2y_1^2)}\right).$$

Принциповими відмінностями кривої (1.5) від (1.1) є циклічна структура групи точок (щодо точок 2-го порядку) і відсутність особливих точок (з діленням на 0 в законі додавання). Останню властивість визначено в [2] як повноту закону складання. Як і для кривої (1.1), зворотна точка визначена як $-(x_1, y_1) = (-x_1, y_1)$, нулем групи точок (нейтральним елементом адитивної групи точок) тут є точка $O = (0, e)$, але існують лише єдина точка 2-го порядку $D = (0, -e)$ і

рівно 2 точки 4-го порядку $\pm F = (\pm e, 0)$.

Важливою є доведена в [2] теорема про повноту закону додавання.

Теорема 1.1 *Для будь-яких пар точок кривої (1.5) знаменники закону додавання (1.6) не звертаються в нуль*: $dx_1x_2y_1y_2 \neq \pm 1$.

Сформульована в теоремі 1.1 властивість автори [2] назвали повнотою закону додавання. У зв'язку з цим в роботі [3] вони віднесли їх до класу *повних кривих Едвардса (complete Edwards curve).*

Справедливість закону додавання (1.6) доводиться наступною теоремою 1.2 [2].

Теорема 1.2 *Нехай* $P = (x, y)$ та $Q = (u, v)$- *точки кривої (1.5) і виконуються рівності точки кривої (1.5) і виконуються рівності*

$$x^2 + y^2 = e^2(1 + dx^2y^2),\ u^2 + v^2 = e^2(1 + du^2v^2).$$

Визначимо

$$X = \frac{(xy+uv)}{e(1+dxyuv)},\ Y = \frac{(yv-xu)}{e(1-dxyuv)},$$

Тоді

$$X^2 + Y^2 = e^2(1 + dX^2Y^2)\ .$$

Треба підкреслити, що рівняння (1.5) містить надмірні параметри. Підстановкою $\frac{x}{e} \to x, \frac{y}{e} \to y$ отримаємо изоморфную криву у формі Едвардса

$$x^2 + y^2 = (1 + d'x^2y^2), \qquad d' = de^4.$$

У такої форми ЕКФЕ, що визначається єдиним параметром d', при додавання точок скорочується кількість операцій на 2 множення в полі. Тому з точністю до ізоморфізмів у формулі (1.5) найчастіше приймають $e = 1$.

1.5 Трансформація еліптичної кривої в формі Вейєрштрасса в форму Монтгомері

У роботах [30,41-42] даний детальний аналіз параметрів a, b кривої (1.7), що породжують ізоморфні криві в формі Монтгомері і Едвардса. Рівняння еліптичної кривої в формі Монтгомері має вигляд

$$M: v^2 = u^3 + Au^2 + Gu,\ A, G \in F_{q.} \qquad (1.10)$$

Нехай c - єдиний корінь кубічного полінома (кубики) в правій частині рівняння (1.7). Тоді це рівняння можна переписати у вигляді

$$Y^2 = (X - c)(X^2 + cX + a + c^2), b = -c(a + c^2). \quad (1.11)$$

З рівності $c^3 + ac + b = 0$ в цьому рівнянні слід, що c - корінь кубики. Заміною $X - c \longrightarrow u,\ Y \longrightarrow v$ отримаємо рівняння в формі Монтгомері (1.10), в якому

$$v^2 = u^3 + 3cu^2 + (a + 3c^2)u \longrightarrow A = 3c,\ G = (a + 3c^2), \quad (1.12)$$

Далі замість пари параметрів a, b буде зручно використовувати параметри a, c , при цьому відповідно до (1.11) $b = -c(a + c^2)$.

Якщо уявити коефіцієнти

$$A = 3c = 2\frac{1 + d}{1 - d}u_1, \quad G = (a + 3c^2) = u_1^2,$$

То рівняння (1.12) приймає вид

$$v^2 = u^3 + 2\frac{1 + d}{1 - d}u_1u^2 + u_1^2u.$$

Визначимо умови, що накладаються на параметри a, c, при яких є єдина точка 2-го порядку і рівно 2 точки 4-го порядку.

Теорема 1.3 *Необхідними і достатніми умовами існування єдиної точки 2-го і двох точок 4-го порядків кривої (1.12) є:*

$a)$ $\chi\big(-(3c^2 + 4a)\big) = -1$, де χ символ Лежандра,

$b)$ $\chi\big(-(3c^2 + a)\big) = 1.$

Умова (a) визначає єдність точки 2-го порядку, а умова (b) - наявність рівно 2-х точок 4-го порядку.

у процесі доказу отримано квадрати для координат точок 4-го порядку

$$u_1^2 = 3c^2 + a = \delta,\ v_1^2 = u_1^2(2u_1 + 3c). \quad (1.13)$$

Звідси випливає, що параметр G в (1.10) та (1.12) повинен бути квадратом, або

$$\chi(\delta) = \left(\frac{(3c^2 + a)}{D}\right) = 1.$$

Другим завданням в цьому розділі буде знаходження залежності між параметрами a та c канонічної форми еліптичної кривої і параметром d кривої $x^2 + y^2 = 1 + dx^2y^2$, у формі Едвардса.

З останнього виразу в (1.13) можна тепер отримати

$$3c = \frac{v_1^2}{v_1^3}\left(1 - 2\frac{v_1^2}{v_1^3}\right)u_1 = 2\frac{1+d}{1-d}u_1,\ d = 4\frac{v_1^2}{v_1^3}. \qquad (1.14)$$

Перша формула в (1.14) дозволяє виразити параметр d через параметри a та c канонічної форми кривої

$$d = \frac{3c-2u_1}{3c+2u_1},\ \ u_1 = (-1)^s\sqrt{3c^2 + a},\ s \in \{0,1\}, \qquad (1.15)$$

Отже, з урахуванням (1.13) і (1.14) коефіцієнти в рівнянні (1.12) дорівнюють

$$A = 3c = 2\frac{1+d}{1-d}u_1,\quad G = (a + 3c^2) = u_1^2.$$

Тоді це рівняння набуває вигляду

$$v^2 = u^3 + 2\frac{1+d}{1-d}u_1u^2 + u_1^2u.$$

Заміною $v^2 \longrightarrow \frac{1}{1-d}v^2$, розподілом правій частині на u_1^3 і заміною $\frac{u}{u_1} \longrightarrow u$ рівняння (1.12) у формі Монтгомері тепер може бути приведене до вигляду, залежному лише від одного параметра d :

$$M\colon \frac{1}{1-d}v^2 = u^3 + 2\frac{1+d}{1-d}u^2 + u. \qquad (1.16)$$

Форма кривої (1.16) за допомогою заміни змінних $(u, v) \longrightarrow (x, y)$ [2, 17] приводиться до ізоморфної кривої у формі Едвардса ($M\square E$).

1.6 Трансформація кривої Монтгомері в ЕКФЕ ті їх ізоморфізми

Пряме і зворотне перетворення координат кривих в формі Монтгомері і формі Едвардса $(u, v) \leftrightarrow (x, y)$ задається раціональними функціями [2]

$$x = 2\frac{u}{v},\quad y = \frac{u-1}{v+1}, \qquad (1.17)$$

$$u = 2\frac{1+y}{1-y},\quad v = 2\frac{1+y}{1-y}x. \qquad (1.18)$$

Множення рівняння (1.16) на $\frac{(1-d)}{u^2}$ дає

$$\left(\frac{u}{v}\right)^2 = (1-d)(u + u^{-1}) + 2(1+d).$$

С урахуванням (1.17) і (1.18) отримаємо

$$\frac{2}{x^2} = (1+d) + (1-d)\frac{1+y^2}{1-y^2} \Longrightarrow$$

$$\Rightarrow 2(1-y^2) = x^2(1-y^2)(1+d) + x^2(1+y^2)(1-d) = 2x^2 - 2dx^2y^2.$$

Звідси отримуємо рівняння ЕКФЕ (1.5) при $e = 1$

$$E: x^2 + y^2 = 1 + dx^2y^2.$$

Рівняння може бути перетворено у рівняння ізоморфної кривої (1.5) з довільним значенням e. Ця крива ізоморфна (чи *біраціонально еквівалентна* [2]) кривої Монтгомері (1.16). Як випливає з цього розділу, на основі раціональних замін координат (1.17) і (1.18) трансформація ($M \square E$) набагато простіше, ніж трансформація з форми Вейєрштрасса ($W \square E$) [МОН].

1.7 Алгоритм побудови ЕКФЕ над простим полем, ізоморфних кривих в формі Вейєрштрасса

Результати, отримані в розділі 1.7, дозволяють побудувати алгоритм обчислення параметрів ЕКФЕ, ізоморфних канонічним еліптичних кривих в формі Вейєрштрасса. Вирішення цього завдання опубліковано в роботах [18, 19].

Завдання полягає у тому, щоб на першому етапі знайти параметри придатної для криптографічних додатків кривій (1.7) у формі Вейєрштрасса, а на другому етапі - розрахувати параметр *d* ізоморфної їй ЕКФЕ.

Згідно з теоремою 1.3, умови існування точок 2-го і 4-го порядків і можна виразити через символи Лежандра як

$a)\quad \chi\left(-(3c^2 + 4a)\right) = -1$, де χ символ Лежандра,

$b)\quad \chi\left(-(3c^2 + a)\right) = 1,\ b = -c(a + c^2).$ (1.19)

Нехай усі параметри не нулеві: $a \neq 0, b \neq 0, c \neq 0$. Таким чином Тем самым мы сразу виключаємо деякі слабкі суперсінгулярні криві. Розглянемо простий приклад.

В умови (1.19) позначимо:

1. При $p \equiv 3 mod 4$

$$\begin{cases} -(3c^2 + 4a) = A^2, \\ 3c^2 + a = B^2, \end{cases} \Rightarrow \begin{cases} a = (3^{-1}(A^2 - B^2), \\ c^2 = 9^{-1}(4B^2 - A^2). \end{cases} \quad (1.20)$$

2. При $p \equiv 1 mod 4$

$$\begin{cases} (3c^2 + 4a)h = A^2, \\ 3c^2 + a = B^2, \end{cases} \Rightarrow \begin{cases} a = (3h)^{-1}(A^2 - hB^2), \ \chi(h) = -1, \\ c^2 = 9^{-1}(4hB^2 - A^2). \end{cases} \quad (1.21)$$

Ці рівності записані на основі (1.19) і властивостей елемента поля, який при $p \equiv 3 mod 4$ є квадратичним нелишком, а при $p \equiv 1 mod 4$ – квадратичним лишком. У зв'язку з цим в рівності (1.21) вписується довільний співмножник h з властивостями квадратичного нелишка.

Формули (1.19) - (1.21) конструктивні, так як дозволяють розраховувати параметри a і $\pm c$ кривої (і відповідно $\pm b$) при заданих значеннях пар квадратичних лишків (A^2, B^2). Об'єктом пошуку є крива порядку $N = 4n$, $n -$ велике просте число. На основі (1.19) - (1.21) можна запропонувати наступний алгоритм побудови канонічних кривих в формі Вейєрштрасса з двома точками 4-го порядку, і далі, ізоморфної ЕКФЕ:

1. В полі F_p задаємо довільне значення пари квадратичних лишків (A^2, B^2) і згідно (1.19) або (1.21) розраховуємо параметри a та c^2. Якщо обчислене значення c^2 не лишок, змінюємо параметр B^2 і повторюємо розрахунки.

2. Якщо обчислене значення c^2 лишок, знаходимо 2 криві з параметрами $(a, \pm c)$ и $(a, \pm b)$. Значення параметра b розраховуємо відповідно до (1.19).

3. Знаходимо координати точки 4-го порядку (для побудови ізоморфної ЕКФЕ).

4. Обчислюємо порядок однієї з кривих і, в разі неприйнятного

порядку, розраховуємо порядок кривої крутіння. Якщо прийнятне рішення не знайдено, переходимо до іншої пари значень (A^2, B^2) (вертаємось в п.1).

5. За формулою (1.15) знаходимо параметр ізоморфної ЕКФЕ.

Даний алгоритм можна модифікувати, фіксуючи, наприклад, параметр c^2, після чого вимагати виконання умов (1.19). Однак у запропонованому вигляді алгоритм швидше призводить до кривої з двома точками 4-го порядку. Далі, як описано в [18], будується ізоморфна ЕКФЕ. У дисертації [20] використаний метод з деякими модифікаціями, що розглянуто вище.

1.8 Кількість ізоморфізмів і пар крутіння кривих Едвардса над простим полем

У деяких криптографічних завданнях, що використовують ізоморфізми, потрібно знати потужність безлічі ізоморфних перетворень або їх оцінки. Для кривих в формі Едвардса над простим полем це завдання вирішується так.

При $e = 1$ кількість різних кривих дорівнює числу квадратичних нелишків d поля $\mu = \frac{p-1}{2}$, тоді загальна кількість різних кривих при всіх значеннях e^2 дорівнює $M = \mu^2$. Відповідно, для кожної кривої з фіксованим d при усіх e^2, є рівно μ ізоморфних кривих. Кількість пар кривих кручення при $p \equiv 1 mod 4$ рівно $\mu/2$, а при $p \equiv 3 mod 4$ - $\frac{(\mu-2)}{2}$. В останньому випадку кількість пар зменшиться на 1, так як при $d = -1$ пара вироджується в одну криву.

Незважаючи на зменшення вчетверо простору всіх кривих і наявність мінімального кофактору 4 у порядку кривої ЕКФЕ безумовно є перспективним напрямком еліптичної криптографії. В першу чергу їх відрізняє найвища серед відомих продуктивність виконання групової операції в проективних координатах [2], універсальність і повнота закону додавання. В існуючих стандартах є канонічні криві з кофактором 4 (зокрема, над полями характеристики 2) [15], тому немає підстав сумніватися в доцільності впровадження технології кривих Едвардса в нові стандарти асиметричної криптографії.

1.9 Аналіз можливості використання детермінованого алгоритму Ель-Гамаля для інкапсуляції ключа

Хоча еліптичні криві є цікавим математичним об'єктом, все ж основний інтерес криптографів зосереджений на їх прикладних властивостях. За останні 20 років еліптичні криві практично витіснили з асиметричної криптографії всі інші алгебраїчні системи, такі як скінченні поля і кільця лишків. Зокрема, існує величезна кількість стандартів цифрового підпису на еліптичних кривих, як міжнародних, так і національних.

Проте на сьогоднішній день у світі існує лише два стандарти, що тією чи іншою мірою стосуються інкапсуляції ключів. Це стандарт Республіки Білорусь СТБ 34.101.45-2013 "Информационные технологии и безопасность. АЛГОРИТМЫ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ И ТРАНСПОРТА КЛЮЧА НА ОСНОВЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ" [22] та міжнародний стандарт ISO/IEC 18033-2 [23].

Зазначимо, що стандарт ISO/IEC 18033-2 був гармонізований і прийнятий як Державний стандарт України ДСТУ ISO/IEC 18033-2:2015. "Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 2. Асиметричні шифри (ISO/IEC 18033-2:2006, IDT)" та введений в дію з 1 січня 2017 року. Він містить короткий опис стандартів ECIES-KEM, PSEC-KEM, ACE-KEM, RSA-KEM.

Проте використовувати зазначений стандарт у реальних ситуаціях для інкапсуляції ключів практично неможливо. Справа у тому, що він не прописує чіткі процедури, які повинні виконуватись для інкапсуляції, а лише наводить певні загальні вимоги до параметрів та функцій, які можуть бути використані для інкапсуляції ключів. А для можливості використання стандарту на практиці у ньому повинні бути прописані абсолютно всі алгоритми, як допоміжні, так і основні, щоб розробники різних організацій, керуючись цим документом, могли створити сумісний програмний продукт.

Що стосується білоруського стандарту СТБ 34.101.45-2013, то тут ситуація інша. У цьому стандарті всі функції та допоміжні алгоритми чітко описані та однозначно визначені. Проте алгоритм інкапсуляції, що в ньому використовується, є дуже громіздким. Більш того, крім операцій у групі точок еліптичної кривої, він використовує також симетричний алгоритм блокового шифрування, який входить до білоруського стандарту блокового шифрування. Використання такого алгоритму суттєво знижує ефективність алгоритму інкапсуляції і викликає багато питань, особливо щодо необхідності використання такої громіздкої структури.

В Україні вітчизняними вченими теж ведуться дослідження з метою впровадження власного Національного стандарту шифрування, який можна було б використовувати на практиці. Перша редакція такого стандарту вже була розміщена на сайтах відповідних державних структур [24] і пройшла обговорення, тепер чекаємо розміщення другої редакції.

Алгоритм, який пропонується в проекті Національного стандарту України, та алгоритм, запропонований у СТБ 34.101.45-2013, не потребують вкладення повідомлення, що передається, у точку кривої. Це можна пояснити тим, що на момент їх створення не було відомо детермінованих алгоритмів вкладення повідомлення у точку, існували лише імовірнісні алгоритми. Тому вибір відповідних алгоритмів для стандарту був досить обмеженим. А якби існували і ефективні детерміновані алгоритми вкладання повідомлення у точку, то для використання у стандарті можна було б також брати Ел-Гамаль-подібні алгоритми [25, 26].

У цьому розділі якраз і будуть отримані результати, що дозволяють будувати ефективні детерміновані алгоритми вкладання повідомлення у точку кривої. На базі отриманих результатів буде показано, як можна побудувати, повністю детермінований, еліптичний аналог алгоритму шифрування Ель-Гамаля.

Взагалі кажучи, для інкапсуляції ключів можна використовувати довільний алгоритм асиметричного шифрування. Один з найпростіших

алгоритмів - алгоритм Ель-Гамаля. Як було зазначено раніше, для використання цього алгоритму на еліптичній кривій нам потрібен алгоритм для вкладення повідомлення (або ключа, якщо мова йде про алгоритм інкапсуляції ключів) в точку на кривій, а також алгоритм для його відновлення з точки. На жаль, до недавнього часу існували лише ймовірнісні алгоритми вкладення. І лише в 2016 році був запропонований детермінований алгоритм, який дозволяв вкладення значення геш-функції у точку кривої. Однак вбудовування ключа є набагато складнішою процедурою, ніж геш-вбудовування. Основні складнощі тут полягають у тому, що це відображення вкладення повинно бути взаємно-однозначним, тобто допускати потім однозначне відновлення ключа з точки кривої. У цьому розділі буде проаналізовано можливість використання згаданого алгоритму для вбудовування ключів та вирішення проблем, що виникають при цьому. Зокрема, буде показано, як можна побудувати не тільки алгоритм вкладення, а й алгоритм однозначного відновлення повідомлення.

Припустимо, сторони A і B, використовують деякий симетричний алгоритм шифрування (наприклад, міжнародний стандарт блокового шифрування AES) для шифрування своїх повідомлень, які будуть потім, у зашифрованому вигляді, надсилатись відкритими каналами від A до B і від B до A. Вони отримують свої секретні ключі від деякого довіреного органу (ДО). ДО генерує ключі, а потім доставляє їх користувачам-кореспондентам. Зазначимо, що таких ключів, індивідуальних для кожної пари користувачів, потрібно багато, вони оновлюються приблизно раз на добу. Тому надсилання ключа кур’єром є практично неможливим, оскільки для цього знадобиться величезна кількість кур’єрів і часто виникатимуть затримки доставки ключа. Найпростіший і, можливо, оптимальний варіант передачі секретного ключа користувачеві A – це зашифрувати його, з використанням деякого асиметричного алгоритму, відкритим ключем користувача A, а потім надіслати його до A через загальнодоступний канал. Аналогічну процедуру з тим самим ключем потрібно зробити і для користувача B. Така процедура називається "інкапсуляцією ключа".

Алгоритми інкапсуляції ключа широко використовуються в сучасній криптографії та представлені в національних та міжнародних стандартах інкапсуляції ключа ISO / IEC [22, 23]. Створення алгоритму інкапсуляції ключів [24], який може використовуватися як національний стандарт, є нині актуальною проблемою. Модифікована схема інтеграції еліптичної кривої (ECIES), включена до стандартів ANSI X9.63, ISO / IEC 18033-2, IEEE 1363a та SECG SEC1, була використана в проекті національного стандарту для шифрування ключа.

Як було зазначено, проблема з використанням "еліптичного" алгоритму Ель-Гамаля [25, 26] полягає у відсутності детермінованих алгоритмів вкладення повідомлення у координату точки кривої. Для використання цього алгоритму на еліптичній кривій потрібні алгоритми для вкладення ключа в точку на цій кривій і для зворотного перетворення. У багатьох роботах, як з теорії чисел, так і з криптології, досліджувалось це питання. Проте до 2016 року існували лише ймовірнісні алгоритми такого вкладення. Вперше алгоритм вкладення геш-значення у точку кривої було запропоновано у роботі [27]. Цікаво, що автори цієї роботи переслідували зовсім іншу мету, ніяк не пов’язану з алгоритмом інкапсуляції. Алгоритм, який вони запропонували, знайшов своє застосування у блокчейні, при реалізації SNARK-доведень без розголошень. У цьому розділі функцію, що використовується у роботі [27] для вкладення геш-значення у точку, буде модифіковано таким чином, щоб отриману модифікацію можна було використовувати у алгоритмі інкапсуляції ключа.

У цьому буде розділі описано, як можна побудувати алгоритм для вкладення повідомлення у точку кривої, а також як побудувати алгоритм для оберненої операції відновлення. Буде показана коректність цих алгоритмів та проаналізована ефективність таких обчислень. У кінці розділу будуть обговорені проблеми, які можуть виникнути при використанні алгоритму вкладення як складової для алгоритму інкапсуляції ключів.

Для формалізації цієї проблеми потрібні наступні позначення.

Розглянемо еліптичну криву $E(F_p)$ над полем F_p, яка задана рівнянням:

$$E: y^2 = g(x),\ \text{де}\ \ g(x) = x^3 + ax + b,\ \ a, b \in F_p, ab \neq 0. \qquad (1.22)$$

Припустимо, що довжина ключа дорівнює n для деякого великого простого числа p де $p > 2^n$. У цьому випадку довільний бітовий вектор k довжини n можна розглядати як двійкове подання деякого елемента$k \in F_p$.

Необхідно побудувати відображення $F_p \to E(F_p)$, яке кожному елементу $k \in F_p$ ставить у відповідність деяку точку $P_k \in E(F_p)$. Більше того, таке відображення повинно бути оборотним, для того, щоб можна було зробити обернене перетворення і відновити ключа з точки.

1.10 Класична криптосистема Ель-Гамаля та її еліптичний аналог

Класична асиметрична схема шифрування Ель-Гамаля була побудована з використанням операцій у мультиплікативній групі F_p^* простого скінченного поля для деякого великого простого p. Її стійкість базується на великій обчислювальній складності розв'язку задачі дискретного логарифмування [28, 29]. Для того, щоб пояснити, в чому саме полягає проблема створення еліптичного аналогу цього алгоритму шифрування, наведемо класичні алгоритми Ель-Гамаля для зашифрування та розшифрування.

Позначимо g генератор мультиплікативної групи F_p^* відповідного простого поля для деякого великого простого числа p.

Нехай секретний ключ абонента А дорівнює a, $2 \leq a \leq p-2$. Тоді відповідний відкритий ключ має вигляд $\square = g^a \ mod\ p$.

Припустимо, що ДО згенерував ключ k (наприклад, для наступному використанні цього ключа для шифрування алгоритмом AES) і тепер повинен доставити його сторонам А і В, використовуючи лише загальнодоступні канали. Припустимо, для шифрування ключа k ДО використовує класичний алгоритм Ель-Гамаля. У цьому випадку ДО робить наступні кроки.

Алгоритм 1.1

Класичний алгоритм Ель-Гамаля (зашифрування ключа)

1. Згенерувати випадкове r, $2 \le r \le p-2$.

2. Обчислити $C_1 = g^r \, mod \, p$.

3. Обчислити $R = \square^r \, mod \, p$.

4. Обчислити $C_2 = k \cdot R \, mod \, p$.

5. Сформувати шифротекст $C = (C_1, C_2)$і надіслати його абоненту А.

Як видно з алгоритму, для зашифрування використовується відкритий ключ абонента А.

Потім ДО виконує ту ж саму процедуру для користувача В, використовуючи відкритий ключ користувача В.

Коли абонент А отримує шифротекст $C = (C_1, C_2)$, він розшифровує його, використовуючи свій секретний ключa, і обчислює зашифрований ключ k, як $k = {C_1}^{-a} \cdot C_2 \, mod \, p$.

Користувач В робить теж саме з переданим йому відповідним шифротекстом, використовуючи свій секретний ключ.

Цю схему можна перетворити на відповідний еліптичний аналог, але існують деякі нюанси. Такий аналог вперше було запропоновано у роботі Кобліца [9]. Але вузьким місцем відповідного еліптичного алгоритму є крок 4 в Алгоритмі 5.1: щоб перенести цей крок на еліптичний випадок, необхідно, щоб k було деякою точкою на еліптичній кривій. Решта кроків алгоритму безпосередньо переносяться на еліптичний обчислення.

Нехай для деякого великого простого числа p базова точка P еліптичної кривої (ЕК) (1.22) $E(F_p)$ має порядок n, де n теж просте. У користувача А є свій секретний ключ a, $2 \le a \le n-2$, і відповідний відкритий ключ $G = aP$. ДО генерує ключ k і повинен доставити його сторонам А і В, використовуючи лише загальнодоступні канали. Припустимо, ДО використовує алгоритм Ель-Гамаля на кривій $E(F_p)$, щоб зашифрувати ключ k, вбудований у точку K на еліптичній

кривій $E(F_p)$. У цьому випадку він робить наступні кроки, що описані в Алгоритмі 1.2:

Алгоритм 1.2

Алгоритм Ель-Гамаля на ЕК (зашифрування ключа)

1. Згенерувати випадкове r, $2 \leq r \leq n-2$.

2. Обчислити $C_1 = rP$.

3. Обчислити $C_2 = K + rG$.

4. Сформувати шифротекст $C = (C_1, C_2)$ і надіслати його абоненту А.

Таку ж саму процедуру ДО робить для користувача В, використовуючи приватний ключ користувача В.

Користувач А отримує шифротекст $C = (C_1, C_2)$ і розшифровує його за допомогою свого секретного ключа a, як $K = C_2 - aC_1$. Користувач В виконує аналогічну процедуру з відповідним шифротекстом, використовуючи свій секретний ключ.

Отже, можна легко побудувати еліптичний аналог алгоритму Ель-Гамаля, за умови існування відповідного алгоритму вкладення повідомлення у точку еліптичної кривої.

У якості такого алгоритму вкладення повідомлення у точку на еліптичній кривій (з наступним відновленням цього повідомлення з точки) Кобліц у [30] запропонував певний імовірнісний алгоритм. Але використання такого алгоритму робить систему дуже складною і незручною. Ось чому еліптичний аналог алгоритму Ель-Гамаля на даний час так і не знайшов свого застосування для інкапсуляції ключів.

Далі було запропоновано інший спосіб побудови алгоритму вкладення. Також буде побудовано алгоритм для відновлення повідомлення та показано коректність цих алгоритмів.

1.11 Побудова алгоритму вкладення повідомлення у точку кривої

Нещодавно в роботі Боне з співавторами [27] було запропоновано детермінований алгоритм для вкладення геш-значення довільної геш-функції в

точку еліптичної кривої. Для побудови алгоритму вбудовування ключа у точку на кривій та для зворотної операції виконаємо деяку модифікацію цього алгоритму.

Нехай еліптична крива $E(F_p)$ задана рівнянням $y^2 = x^3 + ax + b$.

Опис алгоритму Боне:

Нехай для деякої величини $\xi \in F_p$ виконується умова $\xi \notin Q_p$ (тобто елемент ξ поля F_p є квадратичним не лишком цього поля, тут Q_p позначає множину всіх квадратичних лишків поля F_p). Далі, для довільного ключ ключа k, який потрібно зашифрувати, обчислимо величину $u_k = k^2\xi$. Ця величина визначена однозначно для кожної пари kа та ξ. Зауважимо, що u_k теж буде квадратичним не лишком поля F_p, або іншими словами $u_k \notin Q_p$. Тут слід вилучити випадок $u_k = -1$, який може статися лише з нехтувано малою імовірністю (лише за умови $-1 \notin Q_p$і $k^2 \bmod p = -\xi^{-1} \bmod p$).

Тепер знайдемо таке значенняx_k, для якого має місце наступна рівність:

$$g(u_k x_k) = {u_k}^3 g(x_k). \tag{1.23}$$

Рівність (1.23) еквівалентна рівності

$$(u_k x_k)^3 + a u_k x_k + b = {u_k}^3({x_k}^3 + a x_k + b),$$

звідки отримуємо

$$x_k = b(u_k^3 - 1)\left(a u_k (1 - u_k^2)\right)^{-1}. \tag{1.24}$$

Рівність (1.24) можна спростити як

$$x_k = b \cdot \frac{u_k^3 - 1}{a u_k (1 - u_k)^2} = \frac{b(u_k^2 + u_k + 1)}{-a u_k (u_k + 1)} = -\frac{b}{a} \cdot \left(\frac{u_k^2 + u_k + 1}{u_k^2 + u_k}\right) = -\frac{b}{a} \cdot \left(1 + \frac{1}{{u_k}^2 + u_k}\right) \tag{1.25}$$

Для таких x_k отримаємо

$$g(x_k)g(u_k x_k) = g(x_k)u_k^3 g(x_k) =$$
$$= g(x_k)^2 u_k^3 = g(x_k)^2 (k^2\xi)^3 = (g(x_k)k^3\xi)^2\xi$$

Тобто величина $g(x_k)g(u_k x_k)$ є квадратичним не лишком у полі F_p. Це означає, що рівно один з наступних двох елементів $g(x_k)$ та $g(u_k x_k)$ є квадратичним лишком у F_p, а інший є квадратичним не лишком.

Якщо $g(x_k) \notin Q_p$, то для подальших обчислень робимо заміну$x_k \leftarrow u_k x_k$. У цьому випадку для отримання величини u_k використовуємо рівняння (1.26) замість (1.25):

$$\frac{x_k}{u_k} = -\frac{b}{a} \cdot \left(1 + \frac{1}{{u_k}^2 + u_k}\right). \qquad (1.26)$$

Отже, виконується твердження $g(x_k) \in Q_p$, тому існують два квадратних кореня з елемента $g(x_k)$ у полі F_p. Позначимо ці корені $y_{1,2} = \pm\sqrt{g(x_k)}$. Зауважимо, що для одного з коренів $y_{1,2}$ найменший значущий біт дорівнює 0 (тобто $lsb = 0$), а для іншого $lsb = 1$. Тут можна вибрати будь-який з цих двох коренів згідно з деяким заздалегідь визначеним правилом. Наприклад, якщо $lsb = 0$, то покладемо $y_k = y_1$, а якщо $lsb(y_1) = 0$, то $y_k = y_2$. Тоді для отриманої в такий спосіб точки $P_k(x_k, y_k)$ буде виконуватись умова $P_k(x_k, y_k) \in E(F_p)$, для відповідного елемента поля $k \in {F_p}^*$, і таким чином було побудоване відображення $F_p \to E(F_p)$, яке кожному повідомленню (ключу) $k \in {F_p}^*$ однозначно ставить у відповідність деяку точку $P_k(x_k, y_k) \in E(F_p)$.

Загальний вигляд цього відображення, при фіксованому значенні $\xi \notin Q_p$ та значенні і $u_k = k^2\xi$ може бути записаний як

$$P_k = \begin{cases} \left(x_k, \sqrt{g(x_k)}\right), g(x_k) \in Q_p; \\ \left(u_k x_k, \sqrt{u_k^3 g(x_k)}\right), g(x_k) \notin Q_p; \\ \infty, u \in \{-1,0,1\} \end{cases}$$

Наведені вище перетворення є достатніми для побудови та обґрунтування наступного алгоритму вкладення ключа в точку еліптичної кривої.

Алгоритм 1.3

Вкладення ключа в точку еліптичної кривої.

Вхідні дані: $a, b, k, \xi \in F_p$,$\xi \notin Q_p$

1. Обчислити $u_k = k^2\xi$.

2. Обчислити $t_1 = lsb(u_k)$.

3. Обчислити $x_k = -\frac{b}{a}\left(1 + \frac{1}{{u_k}^2 + u_k}\right)$.

4. Обчислити $g_k = {x_k}^3 + ax_k + b; t_2 \leftarrow 0$.

5. Якщо$g_k \notin Q_p$ то $x_k \leftarrow u_k x_k, t_2 \leftarrow 1$ і$g_k \leftarrow {u_k}^3 g_k$.

6. Обчислити $y_{1,2} = \sqrt{g(x_k)}$.

7. Якщо $lsb(y_k) = 1$ то $y_k \leftarrow p - y_k$.

8. Обчислити $t_3 = lsb(k)$.

Вихід: $P_k(x_k, y_k)$, t_1, t_2,t_3.

Тепер залишилось відповісти на питання: як відновити ключ k з заданої точки $P_k(x_k, y_k)$? Відповідь на нього дає можливість побудувати простий еліптичний детермінований алгоритм інкапсуляції ключів на основі алгоритму шифрування Ель-Гамаля.

Зауважимо, що значення t_1, t_2, t_3, в Алгоритмі 1.3 служать саме для вирішення цієї задачі. У наступному підрозділі буде побудовано та обґрунтовано відповідний алгоритм.

1.12 Алгоритм відновлення значення k з точки $P_k(x_k, y_k) \in E(F_p)$

Отже, необхідно побудувати алгоритм обчислення значення k за заданою точкою кривої. Для цього використаємо рівності (1.24) і (1.25). З цих рівностей отримаємо значення u_k як розв'язок відповідного квадратного рівняння. У випадку $g_k \in Q_p$, тобто коли використовується рівність (1.24), отримаємо

$$(u_k{}^2 + u_k)(ab^{-1}x_k + 1) + 1 = 0;$$

$$u_k = \frac{-(ab^{-1}x_k + 1) \pm \sqrt{(ab^{-1}x_k + 1)^2 - 4(ab^{-1}x_k + 1)}}{2(ab^{-1}x_k + 1)};$$

$$u_k = \frac{-1 \pm \sqrt{(ab^{-1}x_k + 1) - 4}}{2};$$

$$u_k = \frac{p-1}{2}(-1 \pm \sqrt{(ab^{-1}x_k - 3)}).$$

У випадку $g_k \notin Q_p$, тобто коли на кроці 5 Алгоритму 1.3 було виконано перетворення $x_k \leftarrow u_k x_k$, отримуємо рівність (1.25). Розв'язуючи відповідне квадратичне рівняння, отримуємо значення u_k:

$$\frac{ab^{-1}x_k}{u_k} + 1 + \frac{1}{u_k(u_k + 1)} = 0;$$

$$u_k{}^2 + u_k(ab^{-1}x_k + 1) + (ab^{-1}x_k + 1) = 0;$$

$$u_k = \frac{-(ab^{-1}x_k + 1) \pm \sqrt{(ab^{-1}x_k + 1)^2 - 4(ab^{-1}x_k + 1)}}{2};$$

$$u_k = \frac{p-1}{2}(ab^{-1}x_k + 1)\left(1 \pm \sqrt{1 - 4(ab^{-1}x_k + 1)^{-1}}\right).$$

Тепер можемо відновити значення k з u_k.

Зауважимо, що саме для однозначного отримання значенняu_k і потрібно було вводити бітові величини t_1, t_2, t_3 у Алгоритмі 1.3. Отже, отримуємо наступний алгоритм для відновлення ключа.

Алгоритм 1.4

Відновлення ключа з точки еліптичної кривої.

Вхідні дані: $x_k \in F_p$, $t_1, t_2, t_3 \in \{0,1\}$.

1. Якщо $t_2 = 0$, то обчислити $u_k = \frac{p-1}{2}\left(-1 \pm \sqrt{(ab^{-1}x_k - 3)}\right)$ і вибрати u_k такий, що $\text{lsb}(u_k) = t_1$, у іншому випадку обчислити $u_k = \frac{p-1}{2}(ab^{-1}x_k + 1)\left(1 \pm \sqrt{1 - 4(ab^{-1}x_k + 1)^{-1}}\right)$ і вибрати u_k такий, що $lsb(u_k) = t_1$.

2. Обчислити $k = \sqrt{-u_k}$

3. Якщо $lsb(k) \neq t_3$, обчислити $k = p - k$.

Вихід: k.

Зазначимо, що отриманий алгоритм інкапсуляції ключів на базі еліптичного алгоритму Ель-Гамаля за складністю обчислень є суттєво ефективніший за білоруський стандарт [22] приблизно аналогічний до проекту стандарту [24].

Ці алгоритми дають можливість використовувати еліптичний алгоритм Ель-Гамаля для інкапсуляції ключів. Такий алгоритм набагато ефективніший (за швидкістю), ніж той, що використовується в національному стандарті Республіки Білорусь для транспорту ключа, і принаймні, не менш ефективний, ніж алгоритм, запропонований в проекті Державного стандарту України національного стандарту шифрування коротких повідомлень (інкапсуляції ключів). Звичайно, для прийняття рішення щодо можливості використання такого алгоритму на практиці, зокрема щодо можливості його стандартизації, потрібний його більш детальний аналіз. Результати аналізу опубліковано [31] і буде темою подальших досліджень.

ВИСНОВКИ ДО РОЗДІЛУ 1

В даному розділі розглядаються сучасний стан еліптичної криптографії та сучасні зміни у сфері використання асиметричної криптографії, загальні проблеми національного стандарту цифрового підпису з яких видно, що стандарт потребує оновлення. Приводяться відгуки провідних спеціалістів з криптографії, з яких можна зробити висновок, що, для створення найбільш криптостійких алгоритмів ЦП, рекомендовано використовувати криптосистеми з використанням ЕКФЕ над простим полем. А також наводяться необхідні основні теоретичні відомості з властивостей ЕКФЕ.

У розділі представлено алгоритм обчислення параметрів ЕКФЕ, ізоморфних канонічним еліптичним кривим в формі Вейєрштрасса та розроблено алгоритм вибору канонічної кривої, ізоморфної ЕКФЕ над простим полем. Також описано залежність між параметром d кривої в формі Едвардса і параметрами ізоморфної їй еліптичної кривої в канонічній формі з параметрами a і b, що забезпечує перехід з однієї форми ізоморфної кривої в іншу.

Наведено основні положення математичного апарату еліптичних кривих у різних формах та представлень, їх взаємозв’язок та властивості. Наведено загальні теоретичні властивості ЕКФЕ. Здійснено трансформацію деяких еліптичних кривих, що використовуються в стандартах ЦП, у форму Едвардса. З метою підтвердження належності ЕКФЕ до еліптичних кривих, як алгебраїчних структур, знайдені та доведені умови ізоморфізму цих кривих і кривих у формі Вейєрштрасса, що дозволяє стверджувати, що ЕКФЕ задовольняють аналогічним вимогам щодо забезпечення безпеки стосовно розв’язання задачі дискретного логарифмування (DLP). За аналізом наявності ізоморфізму приведено теорему щодо визначення точного числа повних кривих Едвардса, ізоморфних кривим у формі Вейєрштрасса з ненульовими параметрами a и b.

Описано два взаємно-обернених детермінованих алгоритми: алгоритм вкладення ключа в точку еліптичної кривої та алгоритм його відновлення з точки. Визначено напрями досліджень дисертаційної роботи..

Перелік використаних джерел до розділу 1

1. Edwards H.M. A normal form for elliptic curves. Bulletin of the American Mathematical Society, Volume 44, Number 3, July 2007, PP. 393-422.

2. Bernstein D.J., Lange T. Faster Addition and Doublingon EllipticCurves // Advancesin Cryptology—ASIACRYPT'2007 (Proc. 13th Int. Conf. On the Theory and Application of Cryptology and Information Security. Kuching, Malaysia. December 2–6, 2007). Lect. NotesComp. Sci. V. 4833. Berlin: Springer, 2007. PP. 29–50.

3. Bernstein Daniel J.,Birkner Peter, JoyeMarc, Lange Tanja, Peters Christiane. Twisted Edwards Curves. //IST Programme under Contract IST–2002–507932 ECRYPT, and in part by the National Science Foundation under grant ITR–0716498, 2008, PP. 1-17.

4. Bernstein Daniel J., Lange Tanja. Farashahi Reza Rezaeian. Binary Edwards curves. Cryptographic hardware and embedded systems–CHES 2008, 10th international workshop, Washington, D.C., USA, August 10–13, 2008, PP. 224-256.

5. Bernstein Daniel J., Batch binary Edwards. Advances in cryptology–Crypto 2009, 29th annual international cryptology conference, Santa Barbara, CA, USA, August 16–20, 2009, PP. 317-336.

6. Bernstein D.J., Lange T. Inverted Edwards coordinates. National Science Foundation under grant ITR–0716498,2007, 331 – 8 and in part by the European Commission through the IST Programme under Contract IST–2002–507932 ECRYPT.

7. Koblitz N., Menezes A.J., A Riddle Wrapped in an Enigma. Technical Reports CACR-2015-14. Available: www.cacr.math.uwaterloo.ca.

8. Moloney R., McGuire G. Two kinds of division polynomials for twisted Edwards curves.ApplicableAlgebrainEngineering, CommunicationandComputing, 2011, PP. 321-345.

9. Bernstein D.J., Birkner P., Lange T., Peters C. ECMusing Edwards curves. European Commission through the ICTProgramme under Contract ICT–2007–216676 ECRYPT-II, and in part by the National ScienceFoundation under grant ITR–0716498.

10. Державний стандарт України ДСТУ 4145-2002.Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих.Формування та перевіряння. Київ, Держстандарт України, 2003. – 94с.

11. ISO/IEC 14888-1,2,3:2008.

12. Державний стандарт України ДСТУISO/IEC 14888-1:2014. Інформаційні технології. МЕТОДИ ЗАХИСТУ. ЦИФРОВІ ПІДПИСИ З ДОПОВНЕННЯМ. Частина 1.Загальні положення. 2014.

13. Державний стандарт УкраїниДСТУISO/IEC 14888-3:2014. Інформаційні технології. МЕТОДИ ЗАХИСТУ. ЦИФРОВІ ПІДПИСИ З ДОПОВНЕННЯМ. Частина 3.Механізми, що грунтуються на дискретному логарифмі. 2014

14. Koblitz N., Menezes A.J., A Riddle Wrapped in an Enigma. Technical Reports CACR-2015-14. Available: www.cacr.math.uwaterloo.ca.

15. Бессалов А.В., Телиженко А.Б. Криптосистемы на эллиптических кривых: Учеб. пособие. – К.: ІВЦ «Політехніка», 2004. – 224с.

16. L. C. Washington. Elliptic Curvres. Number Theory and Cryptography. Second Edition. CRC Press, 2008.

17. Бессалов А.В. Число изоморфизмов и пар кручения кривых Эдвардса над простым полем. Радиотехника, вып. 167, 2011. С. 203-208.

18. Бессалов А.В., Дихтенко А.А., Цыганкова О.В. Алгоритм выбора канонической кривой, изоморфной кривой Эдвардса над простым полем. Радиотехника, №175, 2014.– С.195-198.

19. Бессалов А.В. Построение кривой Эдвардса на базе изоморфной эллиптической кривой в канонической форме. Прикладная радиоэлектроника, 2014, Том 13, №3. – С.286-289.

20. Бессалов А.В., Ковальчук Л.В. Точное число эллиптических кривых в канонической форме, изоморфных кривым Эдвардса над простым полем. Кибернетика и системныйанализ, т.51, №2, 2015.– С.3-12.

21. Дэвенпорт Г. Высшая арифметика: введение в теорию чисел // Пер. с англ. под редакцией Ю.В.Линника. – М: «Наука», 1965. – 176с.

22. СТБ 34.101.45-2013 Информационные технологии и безопасность. Алгоритм электронной цифровой подписи и транспорта ключа на основе эллиптических кривых. Available via https://apmi.bsu.by/resources/std.html/.

23. ISO/IEC 18033-2:2006 Information technology – Security techniques – Encryption algorithms / Part 2: Asymmetric ciphers.

24. Проект національного стандарту Інформаційні технології. Криптографічний захист інформації. Алгоритм шифрування коротких повідомлень, що ґрунтується на скручених еліптичних кривих Едвардса. Available via http://crypton.ua/images/Проект_стандарту.pdf

25. V.Shoup. A Proposal for an ISO Standard for Public Key Encryption. Preprint, December 2001. Available via https://www.shoup.net/papers/iso-2.pdf

26. Wenbo*Mao.* Modern Cryptography*:* Theory and Practice. *PrenticeHall, 2003.707 pp.*

27. Wahby, Riad S. and Dan Boneh. “Fast and simple constant-time hashing to the BLS12-381 elliptic curve.” IACR CryptologyePrintArchive 2019 (2019): 403.

28. P. van Oorschot, S. Vanstone, A. Menezes Handbook of Applied Cryptography, CRC Press, 1996.

29. W. Diffie, M. Hellman “New directions in cryptography.” IEEE Trans. Inform. Theory, vol. IT-22, pp. 472-492, 1976

30. A 9 Neal Koblitz, Elliptic Curve Cryptosystems January 1987, Vol. 48. Number 177. pp. 203-209.

31. Tsygankova O.V. Analyzing of possibility of using Elgamal algorithm with deterministic embedding for key encapsulation» // Радіотехніка, 2020. Вип. № 200 – С. 153-161.

32. *Brown M., Hankerson D., Lopez Jan Menezes A.* Software Implementation of the NIST Elliptic Curves Over Prime Fields. Certicom Research, CORR-2000-56, Canada. www.cacr.math.uwaterloo.ca

33. *Hankerson D., Lopez Jan Meekness A.* Software Implementation of Elliptic Curve Cryptography Over Binary Fields. Certicom Research, CORR-2000-42, Canada. www.cacr.math.uwaterloo.ca.

34. Ann HibnerKoblitz, Neal Koblitz, and Alfred Menezes, Elliptic curve cryptography: The serpentine course of a paradigm shift. CORR-2008-19, Canada. www.cacr.math.uwaterloo.ca.

35. Koblitz N., Menezes A.J., A Riddle Wrapped in an Enigma. Technical Reports CACR-2015-14. Available: www.cacr.math.uwaterloo.ca.

36. Edwards H.M. A normal form for elliptic curves. Bulletin of the American Mathematical Society, Volume 44, Number 3, July 2007, PP. 393-422.

37. Bernstein D.J., Lange T.Faster Addition and Doublingon Elliptic Curves // Advancesin Cryptology—ASIACRYPT'2007 (Proc. 13th Int. Conf. On the Theory and Application of Cryptology and Information Security. Kuching, Malaysia. December 2–6, 2007). Lect. NotesComp. Sci. V. 4833. Berlin: Springer, 2007. PP. 29–50.

38. Bernstein Daniel J., Birkner Peter, Joye Marc, Lange Tanja, Peters Christiane. Twisted Edwards Curves. //IST Programme under Contract IST–2002–507932 ECRYPT, and in part by the National Science Foundation under grant ITR–0716498, 2008, PP. 1-17.

39. Бессалов А.В. Эллиптические кривые в форме Эдвардса и криптография: монография/ А.В.Бессалов. – Киев: КПИ им. Игоря Сикорского, изд-во «Политехника», 2017. – 272с.

40. J. Bos, C. Costello, P. Longa and M. Naehrig, Selecting elliptic curves for cryptography: an efficiency and security analysis, Journal of Cryptographic Engineering, to appear.

41. S. Galbraith and S. Gebregiyorgis, Summation polynomial algorithms for elliptic curves in characteristic two, Progress in Cryptology — INDOCRYPT 2014, LNCS 8885, Springer-Verlag, 2014, pp. 409-427.

42. Semaev, Summation polynomials and the discrete logarithm problem on elliptic curves, available at http://eprint.iacr.org/2004/031.

43. Steven D. Galbraith · PierrickGaudry. Recent progress on the elliptic curve discrete logarithm problem (2016)

РОЗДІЛ 2 НОВА КЛАСИФІКАЦІЯ КРИВИХ В УЗАГАЛЬНЕНОЇ ФОРМІ ЕДВАРДСА ТА ЇХ ВЛАСТИВОСТІ

В даному розділі досліджуються нові властивості кривих в формі Едвардса над простими кінцевими полями характеристики $p > 3$. Проаналізовано властивості точок кривих в узагальненій формі Едвардса малих порядків. Побудована нова класифікація ЕКФЕ і отримані точні формули для кількості таких кривих з порядком $4n$. У розділі запропонована модифікація закону додавання точок кривих з заміною значення координат $(x \leftrightarrow y)$. Введена арифметика для групових операцій з особливими точками цих кривих, дано аналіз точок 2, 4 і 8 порядків і формули, що зв'язують їх з іншими точками кривої. У розділі 2.3 надається аналіз попередніх досліджень щодо класифікації ЕКФЕ і статистики розподілення їх порядків в роботі Bernstein D., Birkner P., Joye M., Lange T., Peters C. Twisted Edwards Curves. // IST Programme under Contract IST–2002–507932 ECRYPT, and in part by the National Science Foundation under grant ITR–0716498, 2008, PP. 1-17. У розділі 2.4 запропоновано нову класифікацію ЕКФЕ в узагальненій формі з розбивкою на три класи, що не перетинаються, в залежності від квадратичності параметрів a і d кривої. Дано аналіз деяких властивостей кривих усіх 3-х класів і можливих значень порядків цих кривих. Далі, у розділі 2.5, описано алгоритм розрахунку точної кількості кривих різних класів з мінімальним кофактором 4 порядку кривої при $p \equiv 1 mod 4$ і $p \equiv 3 mod 4$ та наведено результати .

2.1 Модифікація закону додавання точок кривої в узагальненій формі Едвардса

В роботі [50], з метою збереження горизонтальної симетрії зворотних точок, прийнятої в теорії еліптичних кривих, запропоновано в ЕКФЕ поміняти місцями x і y координати. Спираючись на цю модифікацію, визначимо криву в узагальненій формі Едвардса рівнянням

$$E_{a,d}: x^2 + ay^2 = (1 + dx^2y^2), \quad a, d \in F_p^*, d \neq 1, \ a \neq d, \ p \neq 2. \quad (2.1)$$

Тоді модифікований універсальний закон складання точок кривої (2.1) має вигляд

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1x_2 - ay_1y_2}{1 - dx_1x_2y_1y_2}, \frac{x_1y_2 + x_2y_1}{1 + d\square_1x_2y_1y_2}\right). \quad (2.2)$$

При збігу двох точок отримаємо з (2.2) закон подвоєння точок

$$2(x_1, y_1) = \left(\frac{x_1^2 - ay_1^2}{1 - dx_1^2y_1^2}, \frac{2x_1y_1}{1 + dx_1^2y_1^2}\right). \quad (2.3)$$

Використання модифікованих законів (2.2), (2.3) дозволяє зберегти загальноприйняту горизонтальну симетрію (щодо осі x) зворотних точок. Нейтральний елемент групи кривої в такому вигляді дорівнює $O = (1, 0)$, а зворотна точка: $-P = -(x_1, y_1) = (x_1, -y_1)$.

Тоді отримаємо, згідно (2.1), $(x_1, y_1) + (x_1, -y_1) = (1, 0) = O$. Крім нейтрального елемента O на осі x також завжди лежить точка $D_0 = (-1, 0)$ другого порядку, для якої відповідно до (2.3) $2D_0 = (1, 0) = O$.

Залежно від властивостей параметрів a і d можна отримати ще 2 особливі точки другого порядку і 2 або 4, або 6 точок 4-го порядку. Як випливає з (2.1), на осі y можуть лежати 2 точки $\pm F_0 = (0, \pm 1/\sqrt{a})$ 4-го порядку, для яких $\pm 2F_0 = D_0 = (-1, 0)$. Ці точки існують над полем $\mathbf{F}_p$, якщо параметр a є квадратичним лишком.

Починаючи з цієї глави, будемо використовувати цей модифікований закон складання точок [50].

2.2 Властивості точок порядків 2, 4, 8 кривих в узагальненій формі Едвардса

ЕКФЕ, описані у розділі 2.1, мають просту циклічну структуру з однією точкою 2-го порядку, двома точками 4-го порядку, чотирма точками 8-го порядку і т.д. (за умови їх існування). Рівняння (2.1) може породити криві з більш складною нециклічного структурою точок 2-го порядку, що містять три точки 2-го порядку, від 0 до 8 точок 4-го порядку, до 12 точок 8-го порядку і т.д. Їх аналіз ускладняється тим, що 2 точки 2-го порядку і можливі 2 точки 4-го порядку є особливими, тобто одна з їх координат не визначена в кінцевому полі (що виникає при розподілі на 0).

З рівняння (2.1) визначаємо квадрати координат

$$x^2 = \frac{1-ay^2}{1-dy^2}, \qquad y^2 = \frac{1-x^2}{a-dx^2},$$

в цих виразах особливі точки на нескінченності з'являються при нульових знаменниках:

$$D_{1,2} = \left(\pm\sqrt{\frac{a}{d}}, \infty\right), \quad \pm F_1 = \left(\infty, \pm\frac{1}{\sqrt{d}}\right). \tag{2.4}$$

Такі точки виникають у випадках $\chi(ad) = 1$ та $\chi(d) = 1$ відповідно.

Введемо формальну арифметику з особливими точками (2.4) кривої: позначимо $\infty = \frac{1}{0}$ і $0 = \frac{1}{\infty}$. Поява нескінченної координати в (2.2) або в (2.3) рівнозначно множенню чисельників і знаменників на 0 або 0^2. При цьому залишаються лише складові, які є співмножниками при знаку "∞". Це відповідає правилам граничного переходу. Зокрема, за допомогою закону подвоєння (2.3) можна перевірити, що $2D_{1,2} = 0$, и $\pm 2F_1 = D_0 = (-1, 0)$. Наприклад, в першому випадку

$$2\left(\pm\sqrt{\frac{a}{d}}, \infty\right) = \left(\frac{\frac{a}{d} - a\cdot\infty^2}{1-\frac{da}{d}\infty^2}, \frac{\pm 2\sqrt{\frac{a}{d}}\infty}{1+\frac{da}{d}\infty^2}\right) = \left(\frac{0^2\cdot\frac{a}{d} - a}{0^2 1 - a}, \frac{0\cdot\left(\pm 2\sqrt{\frac{a}{\approx}}\right)}{0^2 1 + a}\right) = (1,0).$$

Іншими словами, при виконанні умов їх існування особливі точки $D_{1,2}$ є точки 2-го порядку, а особливі точки $\pm 2F_1$ – точки 4-го порядку.

Крім перерахованих, точки 4-го порядку можуть існувати як неособливі при ненульових координатах *x* та *y*.

Для аналізу деяких нових властивостей точок 4-го і 8-го порядків [54,56], доведено дві теореми.

Теорема 2.1 *Неособливі точки 4-го порядку*

$$\pm F_2 = \left(\sqrt[4]{\frac{a}{d}}, \pm\sqrt{\frac{-1}{\sqrt{ad}}}\right), \ \pm F_3 = \left(-\sqrt[4]{\frac{a}{d}}, \pm\sqrt{\frac{-1}{\sqrt{ad}}}\right)$$

ЕКФЕ у формі (2.1) *при* $x \neq 0$, *існують тоді і тільки тоді, коли виконуються умови:*

а) при $p \equiv 3 mod 4$: $\chi(d) = \chi(a) = -1$;

?

b) при $p \equiv 1 mo\ \ d4$: $\chi(d) = \chi(a) = 1, \qquad \frac{a}{d} = c^4.$

Доведення

Необхідність. Особливі точки $\pm F_1 = \left(\infty, \pm\frac{1}{\sqrt{d}}\right)$ з формул (2.4), що виникають при $\chi(d) = 1$, виключаються з розгляду відповідно до формулюванням теореми та не розглядаються також точки $\pm F_0 = (0, \pm 1/\sqrt{a})$ при $x = 0$.

Нехай $2F_2 = 2(x_1, y_1) = D_1$. Тоді згідно (2.3) та (2.4) запишемо два рівняння:

$$\frac{x_1^2 - a y_1^2}{(1 - d x_1^2 y_1^2)} = \sqrt{\frac{a}{d}}, \qquad \frac{2x_1 y_1}{(1 + d x_1^2 y_1^2)} = \infty.$$

Звідси $(1 + d x_1^2 y_1^2) = 0, \Rightarrow\ x_1^2 + a y_1^2 = 0, \ \Rightarrow\ x_1^2 = -a y_1^2.$

З $x_1 \neq 0$ випливає $y_1 \neq 0$. Тут друга рівність записана на підставі рівняння (2.1) кривої.

Відповідно до першого з рівнянь і рівності $x_1^2 = -a y_1^2$ маємо

$$\frac{2x_1^2}{1+\frac{d}{a}x_1^4} = \sqrt{\frac{a}{d}} \quad \Rightarrow\ d x_1^4 - 2\sqrt{ad}\, x_1^2 + a = 0 \ \Rightarrow\ x_1^2 = \sqrt{\frac{a}{d}}, \ y_1^2 = -\frac{1}{\sqrt{ad}}.$$

Отже, отримуємо 4 точки з координатами:

$$\pm F_2 = \left(\sqrt[4]{\frac{a}{d}}, \pm\sqrt{\frac{-1}{\sqrt{ad}}}\right), \ \pm F_3 = \left(-\sqrt[4]{\frac{a}{d}}, \pm\sqrt{\frac{-1}{\sqrt{ad}}}\right). \qquad (2.5)$$

При $p \equiv 3 mod 4$ елемент (-1) є квадратичний нелишок [29], тоді $(-a)$ – квадратичний лишок в умовах (а) і рівність $x_1^2 = -a y_1^2$ пов'язує квадрати координат точки F_2.

Нехай β – примітивний елемент мультиплікативної групи $\mathbf{F}_p^*$, и β^2 – квадрат цієї групи, тоді за умови (а) маємо $\beta^2 = \beta^2 \beta^{p-1} = \beta^{2+4k+2} = \beta^{4(k+1)}$. Значить, будь-який квадрат має квадратний корінь і коріння 4-го ступеня при

$p \equiv 3 mod 4$. Необхідність існування перших координат в (2.5) з урахуванням умови (a) доведена.

З огляду на умову (a) і, якщо прийняти значення $\chi(-\sqrt{ad}) = 1$ (тобто як квадратичного нелишка, при цьому $\sqrt{ad}$ – квадратичний лишок), отримуємо по два рішення для інших координат в точках (2.5). Так як квадрати *ad* і *a/d* мають корінь 4-го ступеня, то такі точки в умовах теореми існують. Необхідність умови (a) теореми доведена.

При $p \equiv 1 mod 4$ елемент (-1) є квадратичний лишок [29], тоді рівність $x_1^2 = -ay_1^2$ виконується при $\chi(a) = 1$. Для квадрату мультиплікативною групи маємо $\beta^{\,2} = \beta^2 \beta^{p-1} = \beta^{2+4k} = \beta^{\,2(2k+1)}$ Для цього випадку при $\beta = c^2$ кількість елементів c^4, при всіх ненульових значеннях *c*, рівно $(p-1)/4$.

Обидві координати точок (2.5) існують, якщо $\chi(d) = \chi(a) = 1,$ та $\frac{a}{d} = c^4$. Тоді і для другої координати справедливо $\frac{1}{ad} = \frac{c^4}{a^2} = e^4$. Отже, необхідність умов (b) теореми доведена.

Достатність. Нехай виконуються умови (a) або (b). Тоді існують 4 точки $\pm F_{2,3} = \left(\pm\sqrt[4]{\frac{a}{d}}, \pm\sqrt{\frac{-1}{\sqrt{ad}}}\right)$, для яких згідно (2.3) отримаємо $\pm 2F_{2,3} = D_{1,2}$. Так як подвоєння точок 4-го порядку $F_{2,3}$ дає точки 2-го порядку, то точки, відповідні координатам (2.5) - є точки 4-го порядку. Це доводить достатність умов теореми.

Також точки $\pm F_{2,3}$ можна розглядати як точки поділу на два точок 2-го порядку $D_{1,2}/2$ [57, 58].

Твердження 2.1 *Усі ЕКФЕ* (2.1) *с умовами* $\chi(d) = \chi(a) = -1$ (*при* $p \equiv 1 mod 4$ *мають порядок* $N_E = 4n,$ де $n -$ *непарне*).

Доведення

В умовах $\chi(d) = \chi(a) = -1$ теореми 2.1 при $p \equiv 1 mod 4$ крива не містить точок 4-го порядку, але включає нециклічну підгрупу 4-го порядку точок 2-го порядку $G_4 = \{O, D_0, D_1, D_2\}$. Отже, порядки всіх інших точок можуть бути рівними *n* та $2n$ (разом з можливими непарними співмножниками *n*). Отже, підгрупа G_4 – є

підгрупа мінімального парного порядку 4 кривої і порядок кривої $N_E = 4n$. Твердження доведено.

З твердження 2.1 випливає важливий результат: все скручені ЕКФЕ при $p \equiv 1 mod 4$ мають порядок $N_E = 4n$.

Для визначення умови існування точок 8-го порядку, породжених діленням на 2 точки F_0, докажемо теорему 2.2.

Теорема 2.2 *Необхідними і достатніми умовами існування точок 8-го порядку кривої* (2.1), *породжених діленням на* 2 *точки* F_0, *є:*

(a) *при* $\chi(ad) = -1$: $\chi(a) = 1$, $\chi\left(\frac{d}{a}\right) = 1$;

(b) *при* $\chi(ad) = 1$: $\chi(a) = 1$, $\chi\left(\frac{d}{a}\right) = 1$; та $\chi\left(1 + \sqrt{1 - \frac{d}{a}}\right) = 1$.

Доведення

Необхідність. Нехай $S = (x_1, y_1)$ – точка 8-го порядку, тоді $2S = F_0 = (0, 1/\sqrt{a})$ – одна з точок 4-го порядку на осі *y*. Згідно (2.3) і координат $\boldsymbol{F_0}$ маємо

$$\frac{x_1^2 - a y_1^2}{(1 - d x_1^2 y_1^2)} = 0, \qquad \frac{2 x_1 y_1}{(1 + d x_1^2 y_1^2)} = \frac{1}{\sqrt{a}} \tag{2.6}$$

Тоді $x_1^2 = a$, $\Rightarrow \frac{d}{a} x_1^4 - 2x_1^2 + 1 = 0 \Rightarrow x_{1,2}^2 = \frac{a}{d}\left(1 \pm \sqrt{1 - \frac{d}{a}}\right)$.

Координати точок S_k, k = 1..4, або k = 1..8 визначаються з

$$\boldsymbol{S}_k = \left(\pm \left(\frac{a}{d}\left(1 \pm \sqrt{1 - \frac{d}{a}}\right)\right)^{1/2}, \pm \left(\frac{1}{d}\left(1 \pm \sqrt{1 - \frac{d}{a}}\right)\right)^{1/2} \right). \tag{2.7}$$

Так як справедливо

$$\left(1 + \sqrt{1 - \frac{d}{a}}\right)\left(1 - \sqrt{1 - \frac{d}{a}}\right) = \frac{d}{a}, \tag{2.8}$$

то при $\chi(ad) = -1$ і $\chi\left(1 - \frac{d}{a}\right) = 1$ або $\left(1 + \sqrt{1 - \frac{d}{a}}\right)$ є квадратом, або $\left(1 - \sqrt{1 - \frac{d}{a}}\right)$. Помноживши квадратичний нелишок з цієї альтернативи на нелишок $\frac{a}{d}$, отримаємо значення x_1^2 координати однієї з точок S_k. Отримуючи з квадрата x_1^2 два кореня, визначаємо значення координат $\pm x_1$ в (2.7). Необхідними

умовами існування $\pm x_1$ є умови (a) теореми 2.2. З огляду на умову $\chi(a) = 1$ та $\chi\left(1 - \frac{d}{a}\right) = 1$, розділивши ці значення на $\sqrt{a}$, отримаємо координати $\pm y_1$ точок 8-го порядку. Число точок 8-го порядку, для даного випадку, дорівнює 4. Перше, з необхідних умов теореми 2.2 (a), доведено.

При умові (b) теореми 2.2 $\chi(ad) = 1$ і обидва значення в дужках (2.8) є квадратичні лишки або нелишки. Так як співмножник $\frac{a}{d}$ квадрату x_1^2 є квадратом, то разом з умовою $\chi\left(1 - \frac{d}{a}\right) = 1$ має виконуватися $\chi\left(1 + \sqrt{1 - \frac{d}{a}}\right) = 1$, (і відповідно $\chi\left(1 - \sqrt{1 - \frac{d}{a}}\right) = 1$ Необхідність умов (a) і (b) доведена.

Достатність. Нехай виконуються умови (a) теореми 2.2. Тоді, вибираючи квадратичний не лишок з 2-х значень $\left(1 \pm \sqrt{1 - \frac{d}{a}}\right)$, визначаємо координати 4-х точок з (2.7). Для них $2S = F_0 = (0,1/\sqrt{a})$, тобто в цьому випадку 4 точки 8-го порядку існують.

Нехай виконуються умови (b) теореми 2.2. Так як обидва значення $\left(1 \pm \sqrt{1 - \frac{d}{a}}\right)$ у цьому випадку є або квадратичними лишками, або нелишками, то, з урахуванням $\chi(a) = 1$, отримуємо обидві координати 8-ми точок 8-го порядку (2.7). Збільшення вдвічі числа точок пов'язане з нециклічного структурою точок парного порядку для цього випадку. Отже, 8 точок 8-го порядку в умовах (b) теореми 2.2 існують. Теорема доведена.

Теорема 2.2 не вичерпує всіх можливих точок 8-го порядку, так як при $\chi(ad) = 1$ можуть виникати особливі точки 4-го порядку (2.4) і неособливі точки 4-го порядку (2.5), для яких ділення на 2 може також породити точки 8-го порядку.

За умови існування особливих точок (2.4) разом з точками $D_0 = (-1, 0)$, $\pm F_0 = (0, \pm 1/\sqrt{a}$, приймаючи правила граничного переходу в (2.2), координати сум визначаються як:

$$(x_1, y_1) + (-1, 0) = (-x_1, -y_1),$$

$$(x_1, y_1) + \left(\sqrt{\frac{a}{d}}, \infty\right) = \left(\sqrt{\frac{a}{d}} \cdot x_1^{-1}, \frac{1}{\sqrt{ad}} \cdot y_1^{-1}\right),$$

$$(x_1, y_1) + \left(-\sqrt{\frac{a}{d}}, \infty\right) = \left(-\sqrt{\frac{a}{d}} \cdot x_1^{-1}, -\frac{1}{\sqrt{ad}} \cdot y_1^{-1}\right),$$

$$(x_1, y_1) + \left(\infty, \frac{1}{\sqrt{d}}\right) = \left(-\frac{1}{\sqrt{d}} \cdot y_1^{-1}, \frac{1}{\sqrt{d}} \cdot x_1^{-1}\right),$$

$$(x_1, y_1) + \left(\infty, -\frac{1}{\sqrt{d}}\right) = \left(\frac{1}{\sqrt{d}} \cdot y_1^{-1}, -\frac{1}{\sqrt{d}} \cdot x_1^{-1}\right).$$

Усі знайдені суми задовольняють рівнянню (2.1) при підстановці, тобто є точками кривої.

Використання правил граничного переходу зберігає операцію складання будь-яких пар точок, включаючи особливі. Звідси випливає, що має місце ізоморфізм кривих в формі Монтгомері і Едвардса.

2.3 Аналіз попередніх досліджень щодо класифікації кривих і статистики розподілення їх порядків

У розділі 2 досліджуються нові властивості ЕКФЕ над простими кінцевими полями характеристики $p > 3$. Корисними для криптоалгоритмів можуть бути як різні класи ЕКФЕ над простим полем, так і ЕКФЕ над розширеннями малих простих полів. Для дослідження властивостей ЕКФЕ перш за все необхідно провести їх класифікацію. Авторами роботи [3] була зроблена спроба визначити класи ЕКФЕ. Вона виявилася не зовсім коректною, оскільки породжувала пересічні класи кривих.

В роботі Bernstein D., Birkner P., Joye M., Lange T., Peters C. Twisted Edwards Curves [3], введенням нового параметра a в рівняння (2.1), були визначені с*кручені ЕКФЕ*, як узагальнення ЕКФЕ $x^2 + y^2 = (1 + d'x^2y^2)$ [2]. Поряд з цим, автори [3] не обмежують квадратичність параметрівa і d, допускаючи будь-

які значення $\chi(ad) = \pm 1$. При $a = 1$ така крива отримала в [3] назву *кривої Едвардса*, а якщо $\chi(d) = -1$, то - *повної кривої Едвардса*. Цей термін пов'язаний з повнотою закону додавання точок кривої [2].

Якщо відповідно до вищенаведених визначень позначити клас скручених ЕКФЕ як *TEC*, клас ЕКФЕ як *EC*, а клас повних ЕКФЕ як *CEC*, то має місце включення $CEC \subset EC \subset TEC$. Іншими словами, *повні ЕКФЕ* можна назвати і *кривими Едвардса*, і *скрученими кривими Едвардса*. Виходить, що за класифікацією авторів [3] клас скручених кривих в окремих випадках включає до себе два інших класи, а в клас кривих Едвардса входить підклас повних кривих Едвардса. Це вносить плутанину при вивченні властивостей кривих різних класів. В роботі [3] після спроби класифікувати ЕКФЕ було приведено статистику розподілу порядків кривих різних класів при невеликих значеннях модуля $p = 1009$ та $p = 1019$. Тут з'являється ряд некоректних тверджень авторів [3] і некоректні результати в статистиці розподілу порядків кривих [3, розділ 4].

Для наведеного вище рівняння кривої (2.1), що об’єднує усі три класи, вводимо термін «*криві в узагальненій формі Едвардса*». За термінологією роботи [3] вони визначені як скручені ЕКФЕ. Після проведення складного математичного аналізу, було з'ясовано, що введення нового параметра a в рівняння (2.1) кривої має сенс лише у разі $\chi(d) = \chi(a) = -1$, що дає підставу залишити термін «скручені ЕКФЕ» тільки для цього випадку. Два інших класи ЕКФЕ, за новою класифікацією, ізоморфні кривим з параметром $a = 1$.

2.4 Нова класифікація кривих в узагальненій формі Едвардса

Для розподілу кривих Едвардса на непересічні класи, які мають суттєво різні властивості циклічних і нециклічних груп, в даному розділі запропоновано нову класифікацію кривих в узагальненій формі Едвардса [54,56].

Основні теореми в роботі [3] спираються на біраціональну еквівалентність між кривими (2.1) і кривими в формі Монтгомері

$$M_{A,B}: Bv^2 = u^3 + Au^2 + u, \quad A = 2\frac{a+d}{a-d},\ B = \frac{4}{a-d},\ \square = \frac{A+2}{B},\ d = \frac{A-2}{B},\ A^2 \neq 4.$$

(2.9)

Вона заснована на заміні координат за допомогою раціональних функцій

$$y = \frac{u}{v}, \quad x = \frac{u-1}{u+1} \quad \Rightarrow \quad u = \frac{1+x}{1-x}, \quad v = \frac{u}{y}. \qquad (2.10)$$

В роботі [3] доведено теорему 3.2: *будь-яка скручена крива Едвардса* (2.1) *біраціональна еквівалентної кривої* (2.9) *в формі Монтгомері.*

Так як далі доведеться звертатися до пари квадратичного крутіння (*quadratic twist* [3]), то проведемо відображення точок (2.9) в точки кривої (2.1).

Розділимо рівняння (2.9) на v^2 і з урахуванням (2.10) отримаємо

$$\frac{4}{(a-d)} \cdot \frac{1}{y^2} = u + u^{-1} + 2\ \frac{a+d}{a-d}, \quad \Rightarrow \quad \frac{2}{(a-d)} \cdot \frac{1}{y^2} = \frac{1+x^2}{1-x^2} + \frac{a+d}{a-d}.$$

Звідси

$$\frac{2(1-x^2)}{y^2} = (1+x^2)(a-d) + (1-x^2)(a+d),$$

і, нарешті, отримаємо ізоморфну кривої (2.9) криву в формі (2.1)

$$M_{A,B} \sim E_{a,d}: (1-x^2) = y^2(a-dx^2).$$

Також за допомогою (2.10) можна здійснити і зворотне перетворення. Має місце взаємно однозначне відображення точок $(u_1, v_1) \leftrightarrow (x_1, y_1)$. Якщо для будь-якої пари точок прийняти операцію додавання (2.2) з включенням особливих точок, описаних в п. 2.2, то можна стверджувати, що криві (2.1) і (2.9) ізоморфні:

$$M_{A,B} \sim E_{a,d}.$$

Перейдемо до пар квадратичного крутіння.

Нехай $\chi(c) = -1$, тоді крива крутіння для кривої (2.9) в формі Монтгомері має вигляд

$$M^t_{cB,A}: cBv^2 = u^3 + Au^2 + u, \qquad A = 2\frac{a+d}{a-d}, \quad B = \frac{4}{a-d}.$$

Ізоморфна їй крива в узагальненій формі Едвардса (2.1), як можна бачити з виконаних вище перетворень, записується як

$$E^t_{ca,cd} \sim M^t_{cB,A}: (1-x^2) = cy^2(a-dx^2) = y^2(ca-cdx^2),\ \chi(c) = -1,.$$

Інакше кажучи, для побудови пари квадратичного крутіння до кривої в формі (2.1) слід перейти до нових параметрів кривої (2.1) в формі Едвардса $a' = ca, d' = cd$, при цьому квадратичні нелишки звертаються в нелишки і назад, а квадратичне крутіння кривої (2.1) визначається як

$$E_{a,d}^{t}\sim E_{ca,cd},\ \chi(c)=-1,. \qquad (2.11)$$

У 2-му розділі роботи [3] стверджується, що крива $E_{1,d/a}$ є пара квадратичного крутіння (*quadratic twist*) кривої $E_{a,d}$, т.е. $E_{a,d}^{t}\sim E_{1,d/a}$. Мабуть, слід визнати це твердження в загальному випадку некоректним. Як випливає з аналізу, проведеного вище, воно справедливо лише при $\chi(a)=-1,$, якщо прийняти $c = a^{-1}$. При $\chi(a)=1,$ криві $E_{a,d}$ і $E_{1,d/a}$ ізоморфні: $E_{a,d}\sim E_{1,d/a}$. Тут же автори [3] роблять висновок, що крива $E_{1,d}$ є квадратичне крутіння кривої $E_{1,1/d}$, посилаючись на відомий факт з роботи [2]. Але в [2] це справедливо в умовах $\chi(d)=-1,$ тоді як в [3] допускається $\chi(d)=1,$, і тоді ця пара кривих ізоморфна: $E_{1,d}\sim E_{1,1/d}$ Дійсно, замінивши $d\to d^{-1}$ в рівнянні (2.1) або (2.9) при $a=1$, отримаємо ізоморфну криву за умови $\chi(d)=1,$

Щоб класифікувати криві в узагальненій формі Едвардса з розбивкою на непересічні класи, розглянемо всі 4 поєднання для пар параметрів a і d кривої (2.1). Для цього поставимо їх умовами *C*1 і *C*2 з розбивкою на пари.

***C*1**: $\chi(ad)=-1.$

Існує два варіанти:

***C*1.1**: $\chi(a)=1,\ \chi(d)=-1$ і *C*1.2: $\chi(a)=-1,\ \chi(d)=1.$

Розглянемо перший варіант

***C*1.1** : $\chi(a)=1,\ \chi(d)=-1$

Згідно (2.1) і (2.2) в цьому випадку на кривій (2.1) є єдина точка $D_0=(-1,0)$ 2-го порядку і 2 точки 4-го порядку $\pm F_0 = (0,\pm 1/\sqrt{a})$. Відповідно до (2.10) їм відповідають точки кривої Монтгомері (2.9) $D_{M0}=(0,0)$, $\pm F_{M0} = (1,\pm\sqrt{a})$. Цей випадок описаний в роботі [2]. Тут заміною $(x,y)\to(X,Y/\sqrt{a})$ отримуємо ізоморфну кривої (2.1) повну криву Едвардса $X^2+Y^2=1+d'X^2Y^2$, $\chi(a)=1,$ $\chi(d')=-1$. Отже, для цього випадку має місце ізоморфізм $E_{a,d}\sim E_{1,d/a}$.

Розглянемо другий варіант

***C*1.2**: $\chi(a)=-1,\ \chi(d)=1.$ Тут параметри a і d міняються місцями. За допомогою заміни $(x,y)\to(1/X,Y)$ отримаємо ізоморфну кривої (2.1) криву $X^2+Y^2=1+aX^2Y^2$. Її квадратичне крутіння утворюється заміною $d' = cd,\ a' = ca,\ \chi(\mathrm{c})=-1,$ при цьому $E_{d,a}^{t}\sim E_{\mathrm{cd},ca}$, а це відповідає умові *C*1.1. Згідно *C*1.1

справедливо $E_{d,a}$~$E_{1,a/d}$. Таким чином, пара кривих$E_{d,a}$~$E_{a,d}^{t}$, що відповідають умовам $C1.1$ и $C1.2$, утворюють пару квадратичного крутіння. Цей висновок узагальнює відомий з [2] результат: $E_{1,d}^{t}$~$E_{1,1/d}$.

Таким чином, розглянуті в $C1$ умови для a і d породжують клас ізоморфізмів повних кривих Едвардса, і кожна крива в умовах $C1.1$ заміною $d \to d^{-1}$ відображається в криву квадратичного крутіння $C1.2$ і назад.

Умова друга.

***C*2**: $\chi(ad) = 1$.

Також мають місце два варіанти:

***C*2.1**:$\chi(a) = -1,\ \chi(d) = -1$ і ***C*2.2**:$\chi(a) = 1,\ \chi(d) = 1$.

Розглянемо перший варіант.

***C*2.1**: $\chi(a) = -1,\ \chi(d) = -1$. Згідно (2.9) маємо $(Bad)^2 = (A+2)(A-2)$ і, отже, дискримінант квадратного рівняння в правій частині (2.9) $(A^2 - 4)$ є квадрат. Тоді рівняння$u^3 + Au^2 + B = 0$ має 3 кореня у полі $\mathbf{F}_p$: $\{0, -(A \pm \sqrt{A^2 - 4})/2\}$, а крива Монтгомері містить 3 точки 2-го порядку: $D_{M0} = (0,0), D_{M1,2} = \left(\frac{A \pm \sqrt{A^2-4}}{2}, 0\right)$. Перетворенням координат (2.10) точка D_{M0} кривої (2.9) переходить в точку $D_0 = (-1, 0)$ кривої (2.1), а дві інші точки $D_{M1,2}$ відображаються в 2 точки 2-го порядку $D_{1,2} = \left(\pm\sqrt{\frac{a}{d}}, \infty\right)$ з діленням на 0 y-координати $y = u/v$. Точки 4-го порядку $\pm F_0 = \left(0, \pm\frac{1}{\sqrt{a}}\right)$ на осі y і особливі точки $\pm F_1 = \left(\infty, \pm\frac{1}{\sqrt{d}}\right)$ для цього випадку не існує. Згідно з теоремою 2.1, крива (2.1) має точки 4-го порядку (2.5) лише при $p \equiv 3 \bmod 4$. На основі заміни $(x, y) \to (1/X, Y)$ і множення на X^2 має місце ізоморфізм $E_{a,d}$~$E_{d,a}$.

Другий варіант другої умови

***C*2.2**: $\chi(a) = 1,\ \chi(d) = 1$

Як і в попередньому випадку, є 3 точки 2-го порядку з тими ж координатами, що і в $C2.1$. Крім того, є точки 4-го порядку $\pm F_0 = \left(0, \pm\frac{1}{\sqrt{a}}\right)$ на осі y кривій (2.1).

Разом з тим виникають особливі точки 4-го порядку (2.4) $\pm F_1 = \left(\infty, \pm\frac{1}{\sqrt{d}}\right)$. При $p \equiv 1 \bmod 4$ і $ad = c^4$ відповідно до теореми 2.1 є також 4 точки $\pm F_{2,3}$ (2.5). Значить, є всього 4 або 8 точок 4-го порядку. Для даного випадку перетворення координат $(x, y) \to (X/\sqrt{a}, Y)$ дає ізоморфну кривої (2.1) криву $X^2 + Y^2 = 1 + d'X^2Y^2$, де $d' = d/a$ і має місце ізоморфізм $E_{a,d} \sim E_{1,d/a}$..

З (2.11) вочевидь криві з умовами *C*2.1 і *C*2.2 утворюють пару квадратичного крутіння, тобто $E^t_{a,d} \sim E_{ca,cd}$, $\chi(\mathrm{c}) = -1$,.

На підставі проведеного аналізу властивостей кривих в узагальненій формі Едвардса (2.1) в умовах *C*1 і *C*2 можна зробити висновки:

1. Криві з умовами *C*1 є циклічними повними кривими Едвардса. Заміна умов *C*1.1 на *C*1.2 (або заміна $a \leftrightarrow d$) породжує пару квадратичного крутіння. Ці криві ізоморфні кривим з параметром $a = 1$.
2. Криві з умовами *C*2 є нециклічними кривими Едвардса, що включають 3 точки 2-го порядку, у тому числі дві точки є особливими. Заміна умов *C*2.1 на *C*2.2 (або заміна $a \to ca$, $d \to cd$, $\chi(\mathrm{c}) = -1$,) також породжує пару квадратичного крутіння. Заміна $a \leftrightarrow d$ всередині цих умов породжує ізоморфну криву: $E_{a,d} \sim E_{d,a}$.
3. Криві з умовами *C*2.1 не містять точок 4-го порядку при $p \equiv 1 mod 4$.
4. Криві з умовами *C*2.2 завжди містять 4 або 8 точок 4-го порядку, серед яких 2 точки - особливі.
5. Введення нового параметра a до узагальненої форму кривих Едвардса виправдовується лише виключно в умовах *C*2.1. Всі інші умови призводять до ізоморфним кривим з параметром $a = 1$.

Останній висновок дає підставу для того, щоб термін «*скручені ЕКФЕ*» використовувати лише для кривих з умовами *C*2.1. Разом з тим інші криві, ізоморфні кривим з параметром $a = 1$, логічно розбити на 2 класи: *повні ЕКФЕ* (з параметром $\chi(d) = -1$) і *квадратичні ЕКФЕ* (з параметром $\chi(d) = 1$).

Лише останній термін разом з терміном «*криві в узагальненій формі Едвардса*» є новими в порівнянні з роботою [3], але такі нові визначення класів принципово відрізняються від наведених в роботі [3].

Отже, нова класифікація кривих в узагальненій формі Едвардса (2.1) виглядає таким чином:

- *повні ЕКФЕ* при $\chi(ad) = -1$;
- *скручені ЕКФЕ* при $\chi(a) = \chi(d) = -1$;
- *квадратичні ЕКФЕ* при $\chi(a) = \chi(d) = 1$.

Основні властивості цих трьох класів кривих наведені в таблиці 2.1.

Таблиця 2.1 - Класифікація та властивості кривих в узагальненій формі Едвардса

Умо-ви	Власти-вості	Клас кривих Едвардса	Структу-ра	Точки 2-го порядку	Точки 4-го порядку	ізоморфізм	Клас ізомор-физмів
C1	$\chi(ad) = -1$						
C1.1	$\chi(a) = 1,$ $\chi(d) = -1$	*повні*	*цикліч.*	$\boldsymbol{D_0}$=(−1,0)	$\pm\boldsymbol{F_0}$=(0, $\pm 1/\sqrt{a}$)	$X^2+Y^2=1+d'X^2Y^2$, $d'=d/a \Rightarrow \left(\frac{d'}{p}\right)= -1$ $(x,y)\to(X,Y/\sqrt{a})$	$E_{a,d}$~$E_{1,d/a}$.
C1.2	$\chi(a) = -1$ $\chi(d) = 1$	*повні*	*цикліч.*	$\boldsymbol{D_0}$=(−1,0)	$\pm\boldsymbol{F_0}$=(0, $\pm 1/\sqrt{d}$)	$X^2+dY^2=1+aX^2Y^2$, $d'=cd$, $a'=ca$, $\left(\frac{c}{p}\right) = 1$, $(x,y)\to(1/X,Y/\sqrt{d})$, $X^2+Y^2=1+\frac{a'}{d}X^2Y^2$	$E^t_{1,d/a}$~$E_{1,a/d}$
C2	$\chi(ad) = 1$	**НОВІ КЛАСИ**					
C2.1	$\chi(a) = -1$ $\chi(d) = -1$	*Скручені*	*нецикліч.*	$\boldsymbol{D_0}$=(−1,0) $\boldsymbol{D_{1,\neg}}$= $\left(\pm\sqrt{\frac{a}{d}}, \infty\right)$	$\pm\boldsymbol{F_{2,3}} = \left(\pm\sqrt[4]{\frac{a}{d}}, \pm\sqrt{\frac{-1}{\sqrt{ad}}}\right)$, ($p$≡3mod4)	$(x,y) \to (1/X, Y)$	$E_{a,d}$~$E_{d,a}$
C2.2	$\chi(a) = 1,$ $\chi(d) = 1$	*Квадратичні*	*нецикліч.*	$\boldsymbol{D_0}$=(−1,0) $\boldsymbol{D_{1,2}}$= $\left(\pm\sqrt{\frac{a}{d}}, \infty\right)$	$\pm\boldsymbol{F_0}$=(0, $\pm 1/\sqrt{a}$), $\pm\boldsymbol{F_1}$= $\left(\infty, \pm\frac{1}{\sqrt{d}}\right)$, $\pm\boldsymbol{F_{2,3}}$ = $= \left(\pm\sqrt[4]{\frac{a}{d}}, \pm\sqrt{\frac{-1}{\sqrt{ad}}}\right)$,	$X^2+Y^2=1+d'X^2Y^2$, $d'=d/a \Rightarrow \left(\frac{d'}{p}\right)= 1$, $(x,y)\to(X,Y/\sqrt{a})$	$E_{a,d}$~$E_{d,a}$ $E_{a,d}$~$E_{1,d/a}$ $E_{a,d}$~$E_{1,a/d}$

У розділі 2.4 показано, що криві в оригінальній формі Едвардса ізоморфні кривим $x^2 + y^2 = 1 + e^4x^2y^2$ і, таким чином, при $e^4 = d \neq 1$ відносяться до класу квадратичних кривих Едвардса.

Звернемося до класифікації ЕКФЕ в роботі Bernstein D., Birkner P., Joye M., Lange T., Peters C. Twisted Edwards Curves. [3]. В статистичні таблиці порядків кривих в [3, розділ 4] увійшли в класи кривих Едвардса (*Edwards curve*), повних кривих Едвардса (*complete Edwards curve*) і скручених кривих Едвардса (*twisted Edwards curve*). Як зазначено в розділі 2.1, ЕКФЕ в роботі [3] визначені як $E_{1,d}$ без обмежень на квадратичність параметра *d*. За новою класифікацією це об'єднує два непересічних класи: повних і квадратичних кривих Едвардса. Скручені ЕКФЕ в [3] визначені як криві в узагальненій формі Едвардса (2.1) (за новою запропонованої термінології) і, отже, включають всі три класи, визначені за новою класифікацією. У такому випадку при побудові таблиці розподілу кількості кривих, що входять в різні класи [3], виникає плутанина через те, що одні й ті ж криві будуть враховуватися двічі або тричі.

Через неточною класифікацією в [3] одні і ті ж криві реєструються в різних класах. Наприклад, в таблиці порядків кривих (p=1019) при $p \equiv 3 \bmod 4$ виникає 236 скручених кривих Едвардса з кофактором 4. Цей результат суперечить теоремі 3.4 роботи [3] і доведеною теоремою 2.1 цієї роботи. Значить, вони запозичені з кривих, ізоморфних повним кривим Едвардса, тобто одні й ті ж криві реєструються в різних класах. А це означає, що визначення класів кривих Едвардса, прийняті в [3], в принципі не можуть дати достовірної статистики.

Запропонована нова класифікація кривих в узагальненій формі Едвардса (2.1) з розбивкою їх на 3 непересічних класи є цілком логічною і коректною. Далі в роботі дослідження з використанням нової класифікації [53].

В роботі [3] доведені теореми 3.3 - 3.5 про біраціональних еквівалентності кривих в формі Едвардса і Монтгомері. У теоремі 3.3 [3] доведено, що ЕКФЕ $E1, d$і Монтгомері MA,B біраціональних еквівалентні лише при наявності в них точок 4-го порядку. Далі в теоремі 3.4 [3] доведена біраціональних еквівалентність цих кривих і наявність в них точок 4-го порядку при $p \equiv 3 mod 4$.

Зокрема, для скручених кривих Едвардса (з умовами *C*2.1) порядок кривої $N_E \equiv 0 \bmod 8$. Дійсно, для неї парою квадратичного крутіння є крива з умовами *C*2.2, що має підгрупи 8-го порядку. Отже, її порядок $N_E \equiv 0 \bmod 8N$. Тоді сума числа точок пари кривих крутіння при $p \equiv 3mod4$ дорівнює $N_E + N_E^t = 2(p+1) = 2(4k+3+1)$. Звідси випливає $N_E^t = 0mod8$.

При $p \equiv 1mod4$ аналогічно отримаємо $N_E + N_E^t = 2(p+1) = 2(4k+1+$ $+1)$, тоді $N_E + N_E^t = 0mod4$, і при $N_E = 0mod8$ для квадратичної кривої Едвардса порядок скрученої кривої Едвардса $N_E^t = 0mod4$. В цьому випадку скручена крива має 3 точки 2-го порядку і не має точок 4-го порядку. Це ж стверджує умова (а) теореми 2.1. При цьому немає ізоморфізму скрученої кривої Едвардса з кривою $E1, d/a$, яка має точки 4-го порядку (теорема 3.5 [3]). Отже, скручені ЕКФЕ з мінімальним кофактором 4 порядку $N_E = 4n$ існують лише для половини можливих значень модуля $p \equiv 1mod4$.

При пошуку кривих Едвардса для криптографічних додатків слід шукати криві порядку$N_E = 4n$ з мінімальним кофактором 4 при непарному n, з яких відбираються криві з простим n. Серед повних кривих Едвардса (умови *C*1) практично половина мають порядок $4n$ (n - непарне). Вони є циклічними, і їх порядки пробігають всі кратні 4-м числа в межах Хассе. Квадратичні ЕКФЕ є нециклічними з трьома точками 2-го порядку і чотирма або 8-ю точками 4-го порядку. Звідси випливає, що вони містять нециклічну підгрупу, ізоморфну Z/2×Z/4 порядку 8, а порядок цих кривих має мінімальний кофактор 8. Тому криві порядку $N_E = 4n$, поряд з повними кривими Едвардса, можна шукати лише серед скручених кривих в умовах *C*2.1. Відповідно до твердження 2.1 і наведеного вище аналізу, при $p \equiv 1mod4$ усі скручені криві мають порядок $N_E = 4n$.

2.5 Кількість кривих в узагальненій формі Едвардса порядку 4*n*

Визначивши властивості кривих в узагальненій формі Едвардса, немає сенсу визначати статистику порядків цих кривих, як було зроблено в [3]. На

основі нової класифікації в розділі 2.3 і властивостей кривих знайдемо точне число кривих (2.1) (з точністю до ізоморфізму при $e = 1$) порядку $4n$ (n – непарне) [56]. Для цього розглянемо 2 випадки.

А. ***При*** $p \equiv 1 mod 4$

Для повних кривих Едвардса з умовою *C*.1 число всіх кривих дорівнює числу квадратичних не лишків $(p - 1)/2$. Так як для пари квадратичного крутіння справедливо $N_E + N_E^t = 2(p + 1) = 0 mod 4$, то з $N_E = p + 1 - t = 0 mod 4 N_E$ і $p + 1 \equiv 2 mod 4$ слід $\pm t \equiv 2 mod 4$. При цьому $N_E^t = 0 mod 8$. Отже, якщо порядок однієї з кривих має мінімальний кофактор 4, то порядок кривої крутіння має мінімальний кофактор 8 і навпаки. Оскільки кожній кривій відповідає одна крива крутіння з інверсією $d \to d^{-1}$, то число повних кривих Едвардса з мінімальним кофактором $M_{A1} = M_{1.1} + M_{1.2} = (p - 1)/4$. Тут позначені $M_{i,k}$ – число кривих в класах з умовами *C*.1 до розділу 2.3, $i, k = 1,2$.

Крім цього, при $p \equiv 1 \mathrm{mod} 4$ кривими з мінімальним кофактором 4 є все скручені криві (твердження 2.1). Їх число знайдено за допомогою їх кривих крутіння.

Для кривих з умовами *C*.2.2 класифікації квадратичні ЕКФЕ будуються за допомогою квадратів $\delta = \left(\frac{d}{p}\right)$, з яких викидається 1, так що залишається $(p - 3)/2$ квадратичних лишків. Так як інверсія $\delta \to \delta^{-1}$ дає ізоморфну криву, слід знайти число ізоморфізмів. Так як елемент (– 1) є квадратом при $p \equiv 1 \mathrm{mod} 4$ і збігається зі своєю інверсією, що замість пари ізоморфних кривих породжує одну криву. Тоді число пар ізоморфних кривих одно $(p - 5)/4$. Додаючи до цього числа криву з $\delta = -1$, отримуємо число ізоморфізмів квадратичних кривих Едвардса з мінімальним кофактором 8 $M_{2.2} = (p - 1)/4$. Перехід до скрученим кривим Едвардса з умовами *C*2.1 з мінімальним кофактором 4, як квадратичним крутінням кривих з умовами *C*2.2, дає той же число кривих $M_{2.1} = (p - 1)/4$. Всі скручені ЕКФЕ при $p \equiv 1 \mathrm{mod} 4$ мають порядок $N_E = 4n$. Таким чином, в умовах *C*.2 число кривих з порядком $4n$ дорівнює $M_{A2} = (p - 1)/4$. Загальна кількість

кривих у формі (2.1) порядку $4n$ при $p \equiv 1 \bmod 4$ дорівнює $M_A = M_{A1} + M_{A2} = (p-1)/2$.

В. *При $p \equiv 3 \bmod 4$*

Для цього випадку криві (2.1) порядку $4n$ існують лише в класі повних кривих Едвардса (умови $C1$). Будь-яка крива при цьому містить тільки 2 точки 4-го порядку, і половина кривих – 4 точки 8-го порядку. З $(p-1)/2$ квадратичних не лишків d мультиплікативної групи $\mathbf{F}_p^*$, відповідно до умовою теореми 1.3, слід залишити значення, для яких $\chi(d) = -1$. Іншими словами, слід знайти число пар додатку $d(1-d)$, в яких обидва співмножники - квадратичні не лишки. Подібна задача розглядалась в роботі [44]. Введемо позначення N для квадратичного не лишку, S - для квадратичного лишку, при цьому (NN), (SS), (NS), (SN) – число пар в схемі Гаусса для всіх добутків $m(m+1)$, $m = 1, 2, 3, \ldots, p-1$ [67]. Перепишемо $d(1-d) = -d'(d'+1)$, $d' = d-1$, що відповідає схемі Гаусса. У цій схемі слід знайти число пар (SN), так як $(-d')$ – квадратичний лишок, а $(d'+1)$ – не лишок. Згідно формули (15) в [44] отримаємо шукане число $(SN) = \frac{p-\varepsilon}{4}$, $\varepsilon = (-1)^{\frac{p-1}{2}}$. В даному випадку при $p \equiv 3 \bmod 4$, $\varepsilon = -1$ і $(SN) = \frac{p+1}{4}$. Таким чином, число кривих (2.1) порядку $4n$ для даного випадку $M_B = (p+1)/4$.

Отже, практично половина всіх кривих (2.1) в узагальненій формі Едвардса при $p \equiv 1 \bmod 4$ і чверть їх при $p \equiv 3 \bmod 4$ має мінімальний парний кофактор 4 порядку кривої. Їх число в класі повних кривих Едвардса вдвічі більше, ніж в класі скручених кривих Едвардса.

Можна помітити (таблиця 2.2), що введення нового параметра a в узагальнену форму (2.1) кривої Едвардса лише в 1.5 рази розширює множину кривих в формі Едвардса з мінімальним кофактором 4. Множина скручених кривих з цією властивістю існує лише при $p \equiv 1 \bmod 4$. Так як скручені ЕКФЕ при $p \equiv 1 \bmod 4$ мають порядок $4n$, то це спрощує пошук корисних кривих для криптосистем. Максимальний порядок точки такої кривої дорівнює $2n$, що дозволяє знайти генератор G криптосистеми одним подвоєнням випадкової точки кривої.

Таблиця 2.2 - Точна кількість кривих різних класів з мінімальним кофактором 4 порядку кривої при $p \equiv 1 mod 4$ и $p \equiv 3 mod 4$.

Модуль поля		Клас кривої	Кількість кривих	
A $p \equiv 1 mod 4$	A1 $p \equiv 1 mod 4$	повні	$M_{A1}=(p-1)/4$	$M_A = M_{A1}+M_{A1} = (p-3)/2$
	A2 $p \equiv 1 mod 4$	скручені	$M_{A2}=(p-5)/4$	
B $p \equiv 3 mod 4$		повні		$M_B = (p+1)/4$

Висновок: приблизно 3/8 кривих з мінімальним кофактором порядку кривої 4 можуть бути використані у криптоалгоритмах.

2.6 Метод обчислення точок відомого порядку

Еліптичні криві в формі Едвардса сьогодні є найбільш швидкими і перспективними для використання в асиметричних криптосистемах. Введений Едвардсом в роботі [1] закон складання точок при всіх його перевагах виявився не зручним в еліптичної криптографії, де прийнята горизонтальна симетрія зворотних точок. У цьому розділі внесені корективи до цього закону з метою уніфікації визначення зворотних точок, загальноприйнятого в теорії еліптичних кривих над простим полем.

Симетрія точок кривих Едвардса щодо обох координатних осей тягне за собою цікаві і зручні властивості цих кривих. Виключаючи даремні ізоморфні криві, в кривих Едвардса досить використовувати один параметр d замість звичайних двох параметрів a і b класичної кривої в канонічній формі. Займаючись проблемою розподілу точки кривої на 2, зворотній подвоєння точки, автор [34] виявив умови подільності на 2 для точок кривої великого порядку (більше 4-го).

Умови формулюються і доводяться в теоремі 2.1. У теоремі 2.2 доведено важливу властивість, що зв'язує обидві координати таких точок. При вивченні властивостей кривих були також знайдені вироджені пари кривих крутіння, які

породжують суперсінгулярні криві з порядком (p + 1). В роботі сформульована і доведена теорема 2.3 про необхідні умови існування таких пар кривих крутіння. Доведено також 2 твердження про порядки точок кривої. Далі ми показали на прикладі, як знання всього 1/8 частини точок кривої Едвардса дозволяє реконструювати всі інші точки цієї кривої, задані скалярним твором kP. Така можливість, однак, не спрощує проблеми дискретного логарифмування для точок простого порядку.

Серед загальносистемних параметрів криптосистеми на еліптичних кривих найважливішим елементом є її генератор як точка досить великого простого порядку n. При використанні кривих Едвардса над простим полем порядок кривої $N_E = 4n$, де n - велике просте число [1 - 3]. Після знаходження випадкової точки $Q = (x_Q, y_Q)$ кривої генератор криптосистеми порядку n неважко знайти як точку $G = (x_G, y_G) = 4Q$, для чого буде потрібно два подвоєння (тобто дві групові операції). У розділу показано, що завдання знаходження генератора вирішується простіше - двома операціями в поле і одним подвоєнням в групі точок.

Сімейством точок великого порядку називається 8 точок кривої, що лежать на одному колі з радіусом, більшим 1. У розділі дано аналіз властивостей точок сімейства, на основі яких вдається без групових операцій знаходити точки різних порядків і реконструюватимуть точки скалярного добутку

Ідея і метод визначення порядків точок кривих Едвардса розглядалися в роботі [4]. Для цього було залучено рішення задачі, зворотній подвоєння точки: розподіл точки на 2. У цьому розділі ми наводимо новий підхід до вирішення задачі, зворотній подвоєння точки: розподіл точки на 2, і доводимо необхідну і достатню умову подільності точки на 2. Ця умова дозволила сформувати простий алгоритм обчислення точок необхідного порядку для використання в криптосистемах.

2.6.1 Необхідна і достатня умова подільності точки кривої Едвардса на два

Нехай $P = (x_1, y_1)$ и $2P = (a,b)$. В цьому випадку можна записати зворотну подвоєння (5) точки операцію ділення точки на 2 як $(a,b)/2 = P$. Другим рішенням

операції ділення на 2 буде точка $(a,b)/2 = P + \boldsymbol{D}$, де $\boldsymbol{D}$ – точка 2-го порядку. Згідно (4) $P + \boldsymbol{D} = (-x_1, -y_1) = P^*$. Подвоєння цих двох точок дає один результат $2P = 2P^*$. Ділення на 2 точки адитивної групи має аналогію з витяганням кореня квадратного з елемента мультиплікативної групи поля характеристики $p \neq 2$. З такими операціями зв'язані родинні проблеми дискретного логарифмування. [5].

Скористаємося формулою подвоєння (2.5) при $e = 1$. Виключимо з розгляду 4 базові точки кривої (2.1), що лежать на колі радіуса 1: нуль групи $\mathbf{O} = (1,0)$, точку 2-го порядку $\boldsymbol{D} = (-1, 0)$ и 2 точки 4-го порядку $\pm\boldsymbol{F} = (0, \pm 1)$. Згідно (2.1) другу координату b в (2.5) можна висловити двома формулами

$$\frac{2x_1y_1}{x_1^2+y_1^2} = b, \qquad \frac{2x_1y_1}{1+dx_1^2y_1^2} = b.$$

Визначим $Z = y_1/x_1$, $V = y_1x_1 \neq 0$. Тоді з урахуванням введених позначень для однієї точки P кривої, що не лежить на колі радіуса 1, одночасно справедливі два квадратних рівняння

$$Z^2 - 2b^{-1}Z + 1 = 0, \quad dV^2 - 2b^{-1}V + 1 = 0 \qquad (2.6)$$

с дискримінантами

$$\Delta_1 = 4b^{-2}(1 - b^2), \qquad \Delta_2 = 4b^{-2}(1 - db^2), \qquad (2.7)$$

і рішеннями

$$Z_{1,2} = b^{-1}(1 \pm \sqrt{1 - b^2}), \qquad V_{1,2} = (db)^{-1}(1 \pm \sqrt{1 - db^2})$$

(2.8)

Вищевикладене дозволяє сформулювати і довести наступну теорему.

Теорема 2.1 *Для будь-якої точки (a,b) кривої Едвардса (2.1), що не лежить на колі радіуса 1, існують 2 точки ділення* $(a,b)/2 = \{P, P+\boldsymbol{D}\}$ *тоді і тільки тоді, коли* $\left(\frac{1-b^2}{p}\right) = \rightleftarrows 1$. *При* $\left(\frac{1-b^2}{p}\right) = \rightleftarrows -1$ *точка* (a,b) *на* 2 *не ділиться.*

Доведення

Необхідність. Подвоєння будь-якої точки P з ненульовими координатами відповідно до закону (2.5) породжує єдину точку $2P = (a,b)$, причому координати точок P і $2P$ є рішеннями двох квадратних рівнянь (2.6) в поле $\mathbf{F}_p$. Необхідною умовою існування рішення першого з рівнянь (2.6), як випливає з (5), є те, що

елемент поля $(1 - b^2)$ є ненульовий квадрат в цьому полі, тобто $\left(\frac{1-b^2}{p}\right) = \rightleftarrows 1$. При виконанні цієї умови крім точки P, для якої $2P = (a,b)$, існує ще одна точка $P^* = P + D = (-x_1, -y_1)$, для якої $2P^* = 2P + 2D = (a,b)$, так як $2D = O$. При $\left(\frac{1-b^2}{p}\right) = \rightleftarrows -1$ рівняння (2.6) рішень в поле $\mathbf{F}_p$ не має і точок ділення на 2 не існує. Необхідність умови теореми доведена.

Достатність. Для будь-який не лежачої на одиничному колі точки P кривої (2.1), для якої має місце рівність (2.5), справедливі обидва тотожності (2.6). Досить зажадати, щоб один з Дискримінант (2.7) був квадратичним вирахуванням, з цього відразу слід, що і другий дискримінант є квадратом. Дійсно, нехай (a,b) – точка кривої (2.1). Тоді рівність $a^2 + b^2 = 1 + da^2b^2$ можна записати як $(1 - b^2) = a^2(1 - db^2)$. Звідси очевидно, що для будь-якої точки (a,b) кривої обидві величини $(1 - b^2)$ и $(1 - db^2)$ або є квадратичними лишками, або - не лишками. У першому випадку існують дві точки поділу $(a,b)/2$, у другому точок розподілу не існує.

Достатність умови теореми доведена.

При невиконанні умови теореми для точки (a,b) точок її поділу на 2 $(a,b)/2$ не існує. Це властивість дозволяє без групових операцій знаходити точки максимального порядку $4n$ кривої Едвардса.

Для 4-х базових точок кривої Едвардса $\mathbf{O} = (1,0)$, точки 2-го порядку $\boldsymbol{D} = (-1, 0)$ и точок 4-го порядку $\pm\boldsymbol{F} = (0,\pm1)$ на 2 ділиться зазвичай лише точка $\boldsymbol{D}$, так що $\boldsymbol{D}/2 = \pm\boldsymbol{F}$ (або $\pm2\boldsymbol{F} = \boldsymbol{D}$). Якщо крива не має точок 8-го порядку, то точки $\pm\boldsymbol{F}$ не діляться на 2, в іншому випадку неважко отримати 4 точки 8-го порядку з координатами $(\pm c, \pm c)$, де c є рішення біквадратних рівняння $dc^4 - 2c^2 + 1 = 0$ [3].

У наступній теоремі визначаються нові властивості обох координат точки кривої Едвардса.

Теорема 2.2 *Для будь-який не базової точки* (x_1, y_1) *кривої* (1) *при* $e = 1$ *справедлива рівність* $\left(\frac{1-\overrightarrow{\leftarrow} x_1^2}{p}\right)\left(\frac{1-y_1^2}{p}\right) = \left(\frac{1-d}{p}\right)$.

Доведення

Для точки (x_1, y_1) з урахуванням визначення (2.1) ($e = 1$) визначимо добуток

$$(1 - dy_1^2)(1 - x_1^2) = 1 + dx_1^2y_1^2 - x_1^2 - dy_1^2 = y_1^2 - dy_1^2 = (1 - d)y_1^2 .$$

З доведення теореми 2.1 матеріалів поля $(1 - y_1^2)$ и $(1 - dy_1^2)$ для усіх точок (x_1, y_1) кривої є одночасно квадратичними лишками або не лишками. Тоді з останнього співвідношення відразу слід, що добуток $(1 - y_1^2)(1 - x_1^2)$ є квадратичним невирахувань при $\left(\frac{1-d}{p}\right) = \overrightarrow{\leftarrow} -1$ і навпаки, що і доводить умова теореми.

Теорема 2.2 легко узагальнюється і на ізоморфні криві (1) з параметром $e \neq 1$. Дійсно, за допомогою заміни $u = x/e$, $v = y/e$, $d' = de^4$ отримуємо рівняння ізоморфної (2.1) кривої $u^2 + v^2 = 1 + +d'u^2v^2$. Для нього умова теореми справедливо після заміни $(x,y) \rightarrow (u,v)$ и $d \rightarrow d'$.

Для кривих Едвардса, що не мають точок 8-го порядку, елемент $(1 - d)$ є квадратичним невирахувань [3]. Тоді з теореми 2.2 випливає, що будь-яка небазова точка такої кривої має пару значень $(1- y_1^2)$ і $(1 - x_1^2)$, одне з яких є квадратичний лишок, а інше - квадратичний не лишок. Зокрема, для точки максимального порядку 4n елемент $(1 - y_1^2)$ – квадратичне не лишок, а $(1 - x_1^2)$ – квадратичний лишок.

Визначення координат точок ділення на два розглянуто в попередній роботі [4]. Зауважимо, що при виконанні умови теореми за формулами (2.8) можна знайти всі рішення (2.8) квадратних рівнянь (2.6), після чого визначаються квадрати для координат точок ділення на 2

$$x_1^2 = (V_{1,2}/Z_{1,2}), \qquad y_1^2 = (V_{1,2}Z_{1,2}). \tag{2.9}$$

На відміну від роботи [4], ми тут використовуємо лише одну координату b точки (a,b), яка ділиться на два, з відбором квадратичних лишків (2.9). Результатом повинні бути дві точки $P = (x_1, y_1)$ и $P^* = (-x_1, -y_1)$, для яких $2P = 2P^* = (a,b)$. В силу симетрії першого з рівнянь (2.6) для x_1 и y_1 їх значення можуть помінятися місцями, що вимагає перевірки результату зворотним подвоєнням.

2.6.2 Визначення точок *kP* кривої Едвардса і їх порядків

У криптосистемах прийнятними є ЕКФЕ з мінімальним кофактором 4 порядку кривої $N = 4n$, де n – досить велике просте число ($n > 2^{163}$). Якщо порядок генератора P кривої E_E Ord$P = 4n$, то генератор криптосистеми $G = 4P$ має порядок Ord$G = n$. Точки 8-го порядку відсутні, якщо $(1 - d)$ – квадратичний не лишок [3].

Твердження 2.1 *На кривій Едвардса порядку 4n не існує точок ділення на 2 для точок $< P >$ максимального порядку і точок* $\boldsymbol{F}$ *четвертого порядку, і існують по дві точки поділу на 2 - для всіх інших точок кривої.*

Доведення *Кожній точці kP* кривої відповідає скалярний множник k к елемент кільця цілих чисел Z_N с операціями по модулю $N = 4n$. Всі непарні елементи $k \in \{1, 3, 5,\ldots, 4n - 1\}$ кільцю $\mathbf{Z}_N$, яким відповідають точки кривої максимального порядку $4n$ і порядку 4 ($\pm\boldsymbol{F} = \pm nP$), не діляться на 2 в кільці $\mathbf{Z}_N$. З іншого боку, всі парні елементи кільця $k = 2s$ при розподілі на два по модулю N (або множенні на 2^{-1}) мають два значення s і $s + N/2$, подвоєння яких по модулю N дає знову $2s = k$. Повертаючись до точок kP кривої, робимо висновок, що твердження 2.1 доведено.

Якщо випадкова точка кривої Q має порядок $2n$, то обидві точки поділу на 2 $\{Q/2, Q/2+\boldsymbol{D}\}$ мають максимальний порядок $4n$. мають максимальний порядок $4n$. Дійсно, подвоєння цих точок порядку $4n$ дає одну точку Q порядку $2n$.

Якщо випадкова точка кривої Q має порядок n, то порядки точок ділення на 2 $\{Q/2, Q/2+\boldsymbol{D}\}$ відрізняються вдвічі і мають значення n і $2n$. Наприклад, якщо Ord$(Q/2) = n$, тобто $n(Q/2) = O$, то $n(Q/2 + \boldsymbol{D}) = \boldsymbol{D} \Rightarrow 2n(Q/2 + \boldsymbol{D}) = \mathbf{O}$.

На підставі доведення теореми 2.1 створимо метод знаходження порядку випадкової точки:

Метод знаходження порядку випадкової точки

Для визначення порядку точок кривої Едвардса зовсім не потрібно виконувати складну операцію скалярного добутку nQ. Якщо у випадкової точки кривої $Q = (x_Q, y_Q)$ величина $(1 - y_Q^2)$ – квадратичний не лишок, то $\mathrm{Ord}(Q) = 4n$. В іншому випадку (з ймовірністю 1/2) порядок точки дорівнює n або $2n$. Згідно з теоремою 2.2, якщо $(1 - y_Q^2)$ – квадратичний не лишок, то елемент $(1 - x_Q^2)$ – квадратичний лишок. Міняючи місцями координати x_Q і y_Q , відразу отримуємо точку порядку n або $2n$ властивістю подільності на 2. Подвоєння будь-якої такої точки дає генератор криптосистеми G – точку порядку n. таким чином, для знаходження точки G потрібно всього дві операції в поле і одне подвоєння в групі точок.

2.7 Взаємозв'язок сімейств точок великих порядків. Реконструкція точок kP кривої Едвардса

На основі симетрії восьми точок повної кривої Едвардса $(\pm x_1, \pm y_1)$, $(\pm y_1, \pm x_1)$ сімейства точок, що лежать на одному колі, і формул (2.14)

$$P + D = (x_1, y_1) + (-1, 0) = (-x_1, -y_1) = P^*;$$
$$P + F = (x_1, y_1) + (0, 1) = (-y_1, x_1); \qquad (2.14)$$
$$P - F = (x_1, y_1) + (0, -1) = (y_1, -x_1).$$

пов'язують ці точки, можна побудувати алгоритм знаходження всіх точок скалярного добутку kP точки P, якщо відомий сегмент 1/8 частини всіх точок. Цей метод запропонований в роботі [2]. Проілюструємо прикладом.

Приклад Розглянемо ЕКФЕ з модулем $p = 19$, для якого виконуються обидві умови теореми 2.3 [2]. при $d \in \{-1, 2, 2^{-1}\}$ маємо суперсінгулярні криві з порядком $N_E = p + 1 = 20$. Виключи $(1 - d)$ – квадратичний лишок. Отримуємо дві криві з параметрами $d = 8$ и $d^{-1} = 12$, і дають пару кривих крутіння з порядками 28 і 12 (для них $t = \pm 8$). Точки першої з них представлені на рис. 2.1.

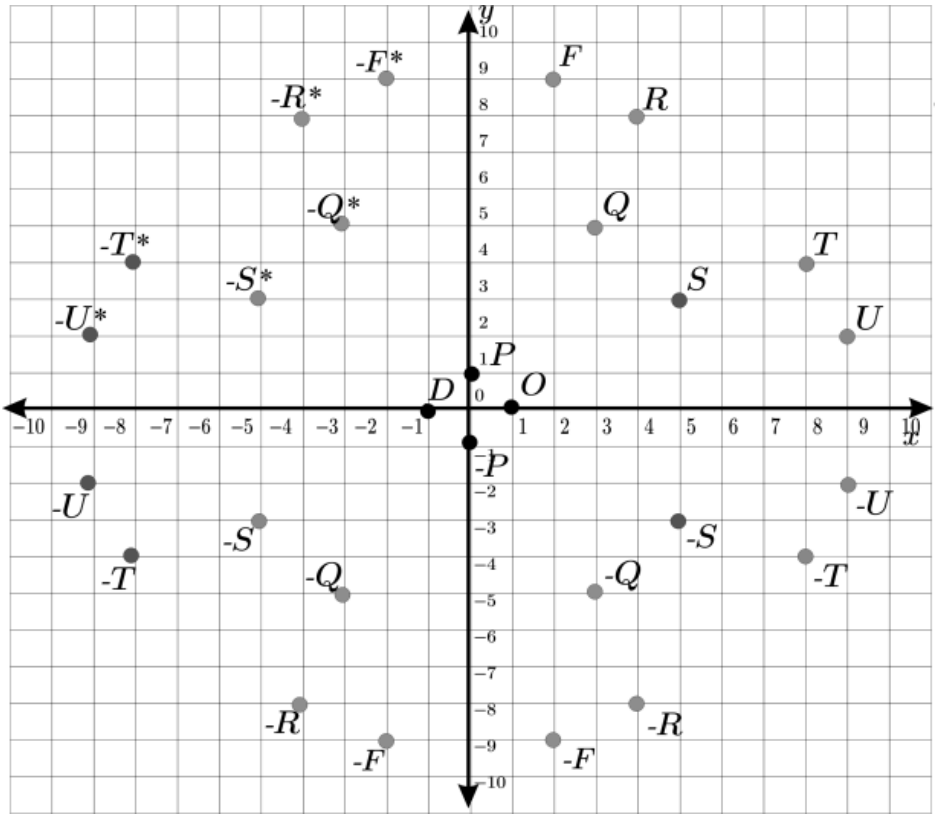


Рисунок 2.1 - Графік повної ЕКФЕ при p = 19, d= 8, N_E= 28

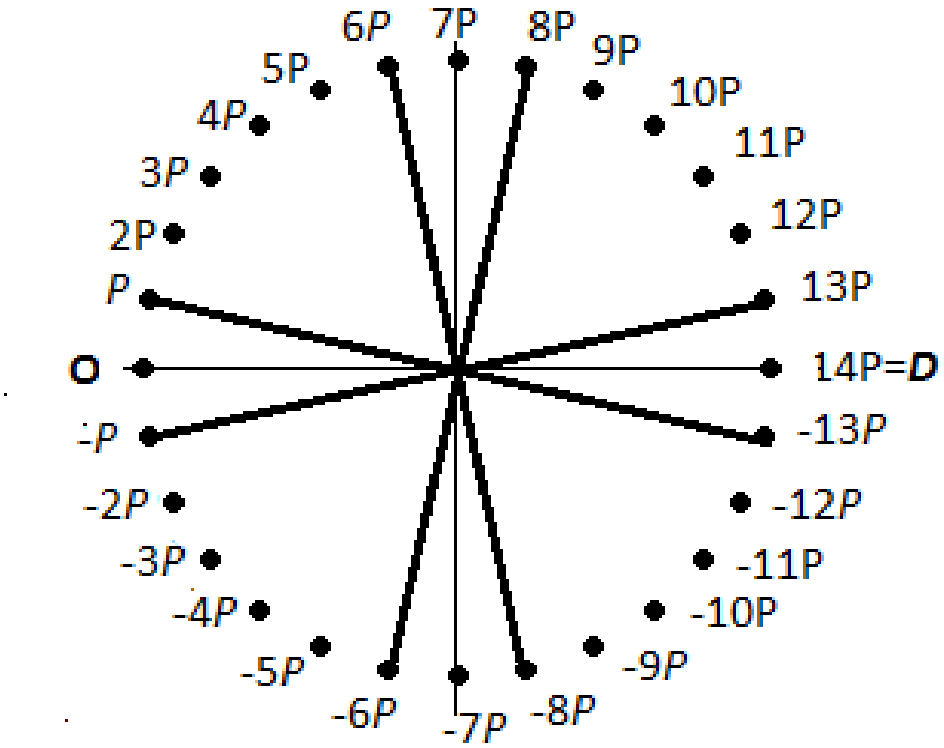


Рисунок 2.2 - Колесо точок циклічної ЕКФЕ порядку N_E= 28

Позначимо P = (2,9), Q = (3,5), R = (4,8), S = (5,3), T = (8,4), U = (9,2) – першого квадранта. Тут точками максимального порядку 28 є точки P, Q, R, для яких значення $(1 - y^2)$ є квадратичними невирахувань. Всіх таких точок $\varphi(28)$ = 12, о 3 точки в кожному квадраті. Крім них, є 6 точок 14-го і 6 точок 7-го порядків. Подвоєння точок P, Q, R дає точки 14-го порядку $2P$ = (–8,4) =–T*, $2Q$ = (–9,2) = –U*, $2R$ = (5, –3) = –S. Отже, в першому квадраті маємо одну точку S 14-го порядку, і 2 точки T і U 7-го порядку.

Циклічну групу точок кривої kP можна представити у вигляді послідовності точок на окружності в порядку зростання скалярного числа k = 0, 1, 2,.., N_E– 1 за годинниковою стрілкою. Для нашого прикладу така точкова окружність представлена на рис. 2.2. Назвемо цей графік колесом Бессалова тому ідея належить йому [6]. Точки колеса Бессалова, з'єднані діаметральними лініями, пов'язані як P і $P^* = P + D$. Для будь-який не базової точки сімейство з 8 пов'язаних лініями точок на рис. 2.2 лежать на одному колі на графіку кривої рис. 2.1.

Знання близько 1/8 частини всіх точок дозволяє реконструювати всі інші точки кривої. Нехай точка P породжує все точки кривої і відомі 4 точки: P = (2,9), $2P$ = (–8,4), $4P$ = (–5,3), $7P$ = –F = (0,–1). В силу властивості $(x_1, y_1) + (-y_1, -x_1) = (0, -1) = -F$, легко знаходяться точки $6P$ = (–9,–2), $5P$ = (–4,8), $3P$ = (–3,5), міняючи місцями координати $x \leftrightarrow y$ і їх знаки відповідно точок P, $2P$ і $4P$. Координати точок kP при k = 0...14 представлені в таблиці 2.3.

Таблиця 2.3 - Координати точок kP повної ЕКФЕ при d= 8, N_E= 28

kP	O	P	$2P$	$3P$	$4P$	$5P$	$6P$	$7P$	$8P$	$9P$	10 P	11 P	12 P	13 P	14 P
x_k	1	2	–8	–3	–5	–4	–9	0	9	4	5	3	8	–2	–1
y_k	0	9	4	5	3	8	–2	–1	–2	8	3	5	4	9	0

Для визначення координат точок правіше точки 4-го порядку ми використовуємо властивість $P + D = P^* = (-x_1, -y_1)$ або $P - P^* = D = 14P$. Наприклад, точка 13P, вертикально симетрична точці P і рівна $-P^*$, має координати $(-x_1, y_1)$. У таблиці 1 добре видно симетрія (антисиметрія) координат точок верхньої половини рис. 2.2: все y-координати симетричні щодо точки $7P$, тоді як x-координати протилежні за знаком. Точки нижньої половини колеса Бессалова рис. 2.2 протилежні точках верхньої половини з інверсією значення y-координати. Наприклад точка $17P = 28P - 11P = -11P = (3,-5)$.

Отже, при відомих 4-х точках (причому одна з них базова $-F$) без обчислень отримали координати всіх 28 точок kP кривої Едвардса. Цей метод годиться для кривої будь-якого порядку, при цьому передобчислювання складаються в розрахунку координат точок kP для $k = 2,3,\ldots,(n-1)/2$, що становить практично 1/8-ю частину порядку кривої. Повертаючись до графіка кривої на рис. 2.1, ми знаходимо в таблиці 2.1 всі її точки як скалярний добуток kP. Точки першого квадранта $Q = (3,5) = 11P$, $R = (4,8) = 9P$ мають порядок 28, точка $S = (5,3) = 10P$ має порядок 14, а дві точки $U = (9,2) = -8P$ і $T = (8,4) = 12P$ – порядок 7. Це відповідає висновкам попереднього аналізу.

Зауважимо, що існує лише 2 точки максимального порядку, які породжують відомий генератор G підгрупи точок простого порядку n– це точки P и P^*, для яких $2P^* = 2P$, $G = 4P$. Всі парні точки колеса рис. 2.2 при переході до породжує точці P^* зберігають свої координати, а непарні $P^*, 3P^*, 5P^*, \ldots$ змінюють знаки обох координат.

Графік точок кривої на рис. 2.1 є точковим і, природно, не відповідає терміну «крива Едвардса» [7]. Якщо послідовно з'єднати прямими лініями точки скалярного добутку $kP, k = 1,2,3, \ldots, N = 28$, то вийде цікава анімація цього графіка кусочно-ламаної кривої. Всього є $\varphi(28) = 12$ точок 28-го порядку, які можуть представити 6 різних графіків (зворотні точки дають один малюнок) це точки

$P^{\langle 1 \rangle} = (2,9)$, $P^{\langle 2 \rangle} = (3,5)$, $P^{\langle 3 \rangle} = (4,8)$, $P^{\langle 4 \rangle} = (-4,8)$, $P^{\langle 5 \rangle} = (-3,5)$, $P^{\langle 6 \rangle} = (-2,9)$. Створені цими 6-ю генераторами графіки представлені на рис. 2.3. [7]

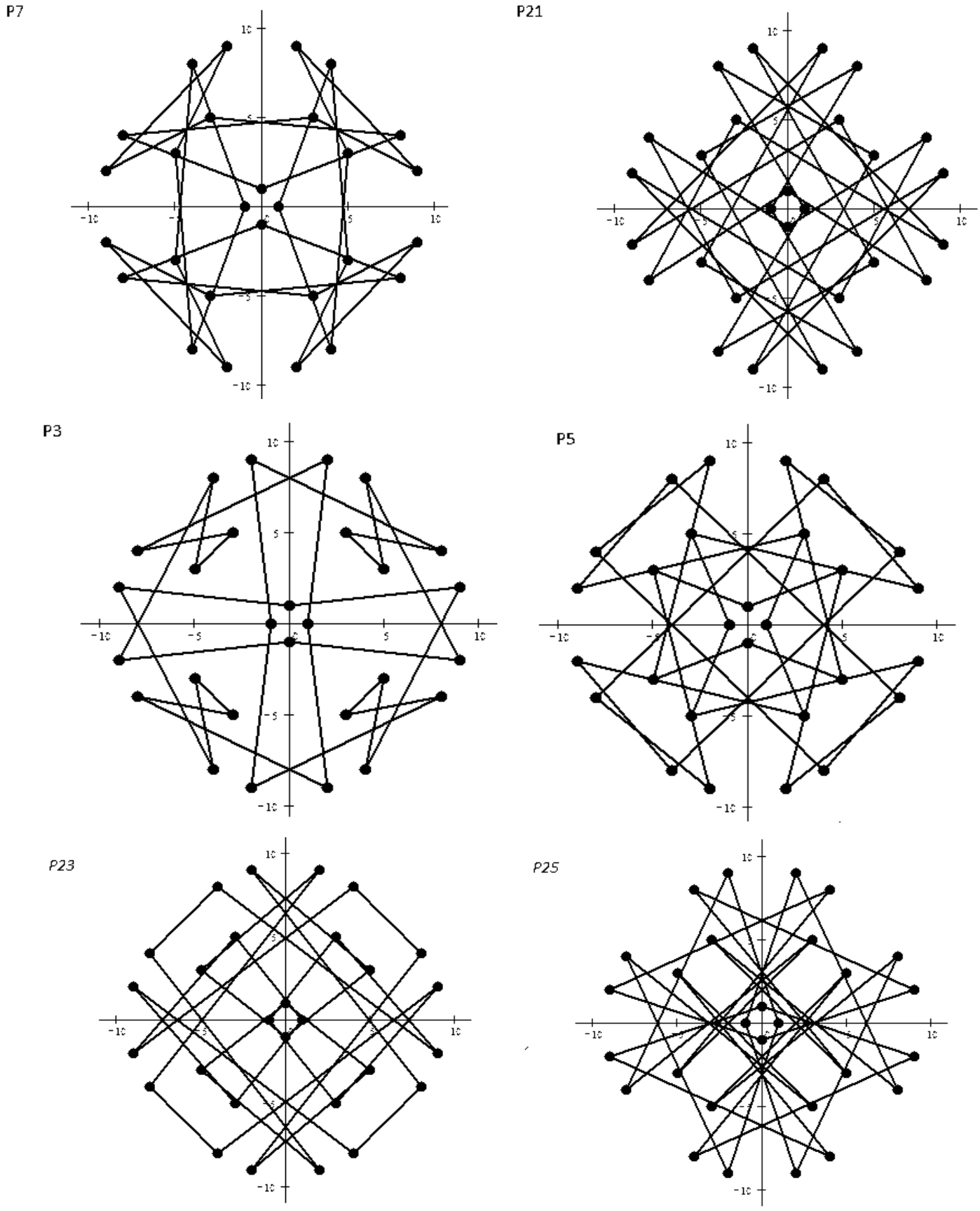


Рисунок 2.3 - Послідовно з'єднані точки скалярного добутку $kP^{\langle i \rangle}$для 6 генераторів $P^{\langle i \rangle}$кривой Едвардса порядку 28 над полем F_{19}

2.8 Порівняльний аналіз швидкості експоненціювання точки ЕКФЕ і кривих у формі Вейерштрасса над кінцевим полем

Автори статті [13], вишукуючи можливості прискорення групових операцій на скручених кривих Едвардса, знайшли цікавий резерв для вирішення цього завдання. Висловивши параметри a і d через координати складаються точок, вони отримали альтернативні формули для законів складання, зокрема

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_1 + x_2y_2}{y_1y_2 + ax_1x_2}, \frac{x_1y_1 - x_2y_2}{x_1y_2 - x_2y_1}\right) = (x_3, y_3) \quad . \tag{2.15}$$

Хоча модифікований закон (2.15) вже в загальному випадку не є повним (існують особливі точки, що звертають знаменники в 0), для точок непарного порядку особливих точок немає і формули (2.15) конструктивні.

Вводячи розширені проектні координати (X: Y: T: Z), авторам [13] вдалося скоротити число операцій у полі при додаванні 2-х різних точок до 9M + 1U (M - множення в полі, S - зведення в квадрат, U - множення на параметр кривої) в порівнянні зі складністю 10M + 1S + 2U при реалізації додавання за формулою (2.2) [1]. Розглянемо їх метод.

При $Z \neq 0$ задаємо чотиривимірні проектні координати (X: Y: T: Z) підстановкою в (2.15) $x = X/Z$, $y = Y/Z$, $t = xy/Z$, $T = XY/Z$. Тоді

$$\frac{X_3}{Z_3} = \frac{(T_1Z_2 + Z_1T_2)}{(Y_1Y_2 + aX_1X_2)}, \qquad \frac{Y_3}{Z_3} = \frac{(T_1Z_2 - Z_1T_2)}{(X_1Y_2 - Y_1X_2)}$$

Звідси

$$\begin{aligned} X_3 &= (X_1Y_2 - Y_1X_2)((T_1Z_2 + Z_1T_2), \\ Y_3 &= (Y_1Y_2 + aX_1X_2)((T_1Z_2 - Z_1T_2), \\ T_3 &= (T_1Z_2 + Z_1T_2)((T_1Z_2 - Z_1T_2), \\ Z_3 &= (Y_1Y_2 + aX_1X_2)((X_1Y_2 - Y_1X_2). \end{aligned} \tag{2.16}$$

Нехай A = X_1X_2, B = Y_1Y_2 , C = T_1Z_2, D = Z_1T_2, E = C + D, F = C – D,

G = B + aA, H = (X_1 – Y_1)(X_2 + Y_2) – A + B $\Rightarrow$

X_3 = EH, Y_3 = GF, T_3 = EF, Z_3 = GH.

Що складність груповий операції додавання різних точок становить VED = 9M + 1U. Якщо параметр $a = \pm 1$ або малий, складність оцінюється як 9M. При подвоєнні точки кривої Едвардса в тривимірних проективних координатах складність подвоєння мінімальна і становить W_{ED} = 3M + 4S + 1U[1]. В роботі [13] в розширених проективних координатах складність подвоєння зростає на одну операцію W_{ED} = 4M + 4S + 1U.

Оцінимо виграш в продуктивності при обчисленні скалярного добутку на скрученої кривої Едвардса в розширених проективних координатах в порівнянні з аналогічною процедурою на канонічній кривої в проективних координатах.

Розрахунок числа операцій при обчисленні суми точок канонічної кривої E дає складність V_E = 12M + 2S. Аналогічний розрахунок для подвоєння точок призводить до результату W_E = 7M + 5S [12] .

Беручи обчислювальну складність зведення в квадрат 1S = 0.67M, а множення на параметр кривої 1U = 0.5м, отримаємо оцінки складності складання і подвоєння на кривій Едвардса V_{ED} = 9.5M, W_{ED} = 4M + 4S + 1U= 7.17M. Для канонічної еліптичної кривої маємо V_E = 13.33M, W_E = 10.33M.

При обчисленні скалярного добутку kP точки P число k представляється в двійковій формі, та використовується алгоритм послідовного складання-подвоєння. Нехай ν – відносна частота знаків 1 в двійковій послідовності k, тоді в загальній формі виграш дорівнює

$$\gamma = \frac{W_E + \nu V_E}{W_{ED} + \nu V_{ED}}. \qquad (2.17)$$

В середньому при рівноімовірно 0 і 1 в двійковій запису числа k ($\nu \to 0.5$) отримуємо середнє значення виграшу$\bar{\gamma}$ = 1.426. що використовувати ЕКФЕ з параметром $a = \pm 1$, то V_{ED} = 9M, W_{ED} = 6.67M і середній виграш досягає значення $\bar{\gamma}$ = 1.521.

У попередньому розділі дана порівняльна оцінка швидкодії операцій на повній кривої Едвардса (a = 1) на основі закону складання (2.2) в проективних

координатах (X: Y: Z), і канонічної кривої. В [1] складність складання точок V_{ED} = 10M + 1S+1U≈11.17M трохи вище, ніж в роботі [13], зате складність подвоєння точок W_{ED}= 3M + 4S = 5.67M менше на одну операцію множення. У підсумку за формулою (2.17) при a = 1 отримуємо середнє значення виграшу $\bar{\gamma}$ = 1.51. Для скрученої кривої Едвардса ($a \neq 1$) при додаванні точок з урахуванням додаткової операції 1U отримуємо середній виграш $\bar{\gamma}$ = 1.48. Отже, втрата продуктивності скрученої кривої Едвардса в порівнянні з повною кривої Едвардса становить близько 2%.

Отже, використання закону складання (2.15) і розширених проективних координат дає вельми незначний приріст продуктивності обчислень на кривій Едвардса в порівнянні з повним універсальним законом складання (2.2). Разом з тим у порівнянні з кривими в формі Вейерштрасса обидві арифметики дають приріст швидкодії приблизно в 1.5 рази.

Якщо використовувати замість двійкового представлення числа k добуток kP трийкове NAF(k) $k_i \in \{0,1,-1\}$[6], то можна знизити середнє число ненульових компонент в числа k до 1/3. За формулою (2.17) при v = 1/3 це дасть максимальне значення середнього виграшу $\bar{\gamma}$ = 1.605 (по методу у роботі [1]) і $\bar{\gamma}$ = 1.531 (по методу у роботі [13]). Тут модифікований закон складання точок [13] вже програє класичному.

2.8.1 Складність групових операцій ЕКФЕ та її мінімізація

Розглянемо в цьому розділі повні ЕКФЕ з параметром a= 1 и $\left(\frac{d}{p}\right) = -1$.

У найбільш загальному вигляді повна крива Едвардса над кінцевим полем $F_q(q = p^m)$ характеристики $p > 3$ може бути виражена як [1]

$$E_E: \quad x^2 + y^2 = c^2\left(1 + \tilde{d}x^2y^2\right), \quad \tilde{d} = c^{-4}d, \tilde{d}(1 - \tilde{d}c^4) \neq 0, \tilde{d} \neq A^2. \quad (2.16)$$

Закон додавання двох точок цієї кривої при вертикальній симетрії зворотних точок має вигляд

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + x_2y_1}{c(1+\tilde{d}x_1x_2y_1y_2)}, \frac{y_1y_2 - x_1x_2}{c(1-\tilde{d}x_1x_2y_1y_2)}\right). \quad (2.17)$$

Варіювання параметра з дає ізоморфні криві, тому з точністю до ізоморфізму можна вважати $c = 1$, $\tilde{d} = d$. Наявність 2-х інверсій в (2.16) змушує звертатися до проектних координатах [12]. Введемо третю координату Z як спільний знаменник в (2.17). Вважаємо $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$, тогда гомогениосное уравнение кривої (2.16) в проективних координатах має вигляд

$$(X^2 + Y^2)Z^2 = Z^4 + dX^2Y^2.$$

Сума двох точок тепер записується як

$$(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2) = (X_3 : Y_3 : Z_3).$$

З урахуванням підстановок висловимо координати сумарною точки згідно (2.17)

$$x_3 = \frac{X_3}{Z_3} = \frac{\left(\frac{X_1Y_2}{Z_1Z_2} + \frac{X_2Y_1}{Z_1Z_2}\right)\left(1 - d\frac{X_1X_2Y_1Y_2}{Z_1^2Z_2^2}\right)}{\left(1 + d\frac{X_1X_2Y_1Y_2}{Z_1^2Z_2^2}\right)\left(1 - d\frac{X_1X_2Y_1Y_2}{Z_1^2Z_2^2}\right)} =$$

$$= \frac{Z_1Z_2(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2)(X_1Y_2 + X_2Y_1)}{(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2)(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2)}$$

$$y_3 = \frac{Y_3}{Z_3} = \frac{Z_1Z_2(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2)(X_1Y_2 - X_2Y_1)}{(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2)(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2)}$$

Позначимо:

$$A = Z_1Z_2;\ B = A^2;\ C = X_1X_2;\ D = Y_1Y_2;\ E = dCD;\ F = B - E;\ G = B + E$$

Тоді

$$X_3 = A \cdot F \cdot ((X_1 + Y_1) \cdot (X_2 + Y_2) - C - D),$$
$$Y_3 = A \cdot G \cdot (D - C),$$
$$Z_3 = F \cdot G.$$

Ігноруючи просту операцію складання (вирахування) в поле, знаходимо складність обчислення суми різних точок V_{ED}= 10M + 1S + 1U. Заметім, що складність зведення в квадрат оцінюється приблизно як $1S \cong \frac{2}{3}M$ [1].

Подібним же чином визначається складність подвоєння точки як W_{ED}= 3M + 4S. Економія в обчисленнях тут досягається заміною згідно (2.1) знаменників в (2.17): $(1 + dx_1^2 y_1^2)$ на $(x_1^2 + y_1^2)$, а $(1 - dx_1^2 y_1^2)$ – на $(2 - (x_1^2 + y_1^2))$.

2.8.2 Складність груповий операції для кривої в формі Вейерштрасса

Звернемося тепер до канонічної еліптичної кривої над полем F_q

$$E: \qquad y^2 = x^3 + ax + b,$$

с законом складання різних точок [12]

$$(x_1, y_1) + (x_2, y_2) = \left(\left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2 , - y_1 - \left(\frac{y_2 - y_1}{x_2 - x_1} \right) (x_3 - x_1) \right)$$

В проектних координатах з заміною $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$ маємо

$$\frac{\frac{Y_2}{Z_2} - \frac{Y_1}{Z_1}}{\frac{X_2}{Z_2} - \frac{X_1}{Z_1}} = \frac{u}{v}. \quad u = Y_2 Z_1 - Y_1 Z_2, \qquad v = X_2 Z_1 - X_1 Z_2.$$

Тоді

$$\frac{X_3}{Z_3} = \left(\frac{u}{v} \right)^2 - \frac{X_1}{Z_1} - \frac{X_2}{Z_2} = \frac{Z_1 Z_2 u^2 - v^2 (X_1 Z_2 + X_2 Z_1)}{Z_1 Z_2 v^2} = \frac{vg}{Z_3},$$

де

$$Z_3 = Z_1 Z_2 v^3, \qquad g = Z_1 Z_2 u^2 - v^3 - 2v^2 X_1 Z_2.$$

Далі

$$\frac{Y_3}{Z_3} = -\frac{Y_1}{Z_1} + \left(\frac{u}{v}\right)\left(\frac{X_1}{Z_1} - \frac{vg}{Z_1 Z_2 v^3}\right) = \frac{-Y_1 Z_2 v^3 + u(X_1 Z_2 v^2 - g)}{Z_1 Z_2 v^3}$$

Маємо

$$X_3 = vg,$$

$$Y_3 = -Y_1 Z_2 v^3 + u(X_1 Z_2 v^2 - g),$$

$Z_3 = Z_1 Z_2 v^3$.

Розрахунок числа операцій дає складність обчислення суми точок канонічної кривої EV_E= 12M + 2S. Аналогічний розрахунок для подвоєння точок призводить до результату [12]W_E= 7M + 5S.

2.8.3 Порівняння швидкості експоненціювання точки для кривих E_E і E

Оцінимо виграш у часової складової при обчисленні скалярного добутку на скрученої кривої Едвардса в проективних координатах в порівнянні з аналогічною процедурою на канонічній кривої в проективних координатах [10].

Розрахунок числа операцій при обчисленні суми точок канонічної кривої *E* дає складність V_E= 12M + 2S. Аналогічний розрахунок для подвоєння точок призводить до результату W_E= 7M + 5S [12].

Беручи обчислювальну складність зведення в квадрат 1S = 0.67M [1], а множення на параметр кривої 1U = 0.5M, отримаємо оцінки складності складання і подвоєння на кривій Едвардса V_{EE}= 11.17M, W_{EE}= 3M + 4S = 5.66M. Подвоєння, як бачимо, значно швидше складання. Для канонічної еліптичної кривої маємо V_E= 13.33M, W_E= 10.33M.

При обчисленні скалярного добуток *kP* точки *P* число *k* представляється в двійковій формі, тоді зазвичай користуються алгоритмом послідовного подвоєння-складання [12]. На кожному кроці експоненціювання *kP* проводитися подвоєння, а операція додавання виконується лише при знаку 1 в двійковій запису числа *k*. Нехай *v* - питома вага Лемінга в двійковому поданні числа *k*, тоді

в загальній формі виграш у швидкодії експоненціювання для повної кривої Едвардса в порівнянні з кривою в формі Вейерштрасса дорівнює

$$\gamma(\nu) = \frac{W_E + \nu V_E}{W_{ED} + \nu V_{ED}}. \qquad (2.18)$$

В середньому при рівноймовірно 0 і 1 в двійковій запису числа k ($\nu \approx 0.5$) отримуємо середнє значення виграшу $\bar{\gamma}$ = 1.51. Якщо використовувати ЕКФЕ з малим параметром d, то ігноруючи множення 1U = 0.5M отримаємо V_{EE}= 10.66M, W_{EE}= 5.66M і середній виграш досягає значення $\bar{\gamma}$= 1.546.

Якщо використовувати замість двійкового представлення числа k добуток kP трийкове NAF(k) $k_i \in \{0,1,-1\}$[12], то можна знизити середнє число ненульових компонент в числі k до 1/3. За формулою (2.7) при ν= 1/3 це дає значення середнього виграшу $\bar{\gamma}$= 1.576. Прі використанні малих параметрів d з економією множення 1U отримуємо максимальний середній виграш $\bar{\gamma}_{max}$ = 1.605.

За результатами аналізу кількості операцій в групі для точок повної та скрученої ЕКФЕ в проективних координатах та на кривій Вейєрштрасса (таблиця 2.2) визначено, що у загальному випадку найменших обчислювальних витрат вимагають операції на повних ЕКФЕ. Особливо повні ЕКФЕ виграють при подвоєнні, яке обходиться без операції множення на параметр кривої. Також, з метою зменшення кількості операцій в групі точок ЕКФЕ, було запропоновано метод досягнення мінімальної складності операцій, який полягає у фіксації параметру a мінімальним значенням 2 або 3 (a = 2 → одне додавання, a = 3 → два додавання у групі точок) та вибором мінімального параметру d, що забезпечує порядок $4n$ кривої з мінімальним кофактором 4, де n – просте. При застосуванні запропонованого методу, з'являється можливість зменшити складність додавання у групі точок через зневагу складності виконання 1U, як малим числом.

Таблиця 2.4 - Кількість операцій в групі точок ЕКФЕ та Вейєрштрасса, де M – множення у полі, S – піднесення до квадрата, U – множення на параметри a та (або) d для точок кривої

Клас кривих	Кількість операцій в полі для однієї групової операції		Оцінка складності при 1S = 2/3M; 1U = 1/2M	
	Додавання точок	Подвоєння точок	Додавання точок	Подвоєння точок
Повні ЕКФЕ	10M +1S+1U	3M+4S	11.17M	5.67M
Скручені ЕКФЕ	10M+1S+2U	3M+4S+1U	11.67M	6.17M
Криві у формі Вейєрштрасса	12M + 2S	7M+5S	13.34M	10.33M
Кількість операцій з використанням запропонованого методу зменшення складності операцій				
Повні та скручені ЕКФЕ	$M + 1S$	$M + 4S$	10.67M	5.67M

Виконані дослідження дозволили з'ясувати, що у повних і скручених кривих Едвардса, для експоненціювання точки, використовується менша кількість операцій ніж у кривих у канонічній формі Вейєрштрасса (таблиця 2.4), що у результаті значно прискорює швидкість експоненціювання точки.

На наступному кроці було проведено порівняльний аналіз складності експоненціювання точки на скрученій і повній кривій Едвардса у порівнянні з кривою у формі Вейєрштрасса. Для цього було застосовано отримані оцінки складності додавання і подвоєння:

на кривій у формі Вейєрштрасса: V_W= 13.33M, T_W= 10.33M,

на повної ЕКФЕ: $V_{E\text{пов}} = 11.17\text{M}$, $T_{E\text{пов}} = 5.67\text{M}$,

на скрученої ЕКФЕ: $V_{E\text{скр}} = 11.67\text{M}$, $T_{E\text{скр}} = 6.17\text{M}$.

За аналізом складності операцій додавання і подвоєння точок на різних кривих визначено коефіцієнт виграшу $\gamma(\nu)$ у складності експоненціювання точки на повної і скрученої ЕКФЕ у порівнянні з кривою у формі Вейєрштрасса:

$$\gamma_{\text{пов}}(\nu) = \frac{10.33+\nu\cdot 13.33}{5.67+\nu\cdot 11.17}, \qquad \gamma_{\text{скр}}(\nu) = \frac{10.33+\nu\cdot 13.33}{6.17+\nu\cdot 11.67}$$

де ν– відносна частота знаків «1» в двійковому (трійковому) зображенні числа k у скалярному добутку kP.

Також знайдено максимальний виграш у складності експоненціювання точки для повної і скрученої ЕКФЕ з застосуванням запропонованого методу досягнення мінімальної складності операцій у групі:

$$\gamma_{\text{max}}(\nu) = \frac{10.33+\nu\cdot 13.33}{5.67+\nu\cdot 10.67}.$$

Результати розрахунку виграшу у складності експоненціювання точки ЕКФЕ у порівнянні з експоненціювання точки кривої у формі Вейєрштрасса було представлено у таблиці 2.5.

Таблиця 2.5 - Результати оцінок виграшу у кількості операцій складності експоненціювання точки для повної і скрученої ЕКФЕ у порівнянні з кривою у формі Вейєрштрасса (в дужках - значення максимального виграшу при мінімальної складності операцій у групі)

Клас кривих	Виграш $\gamma(\nu)$ *де* k – скалярний множник генератора криптосистеми	
	(ν=0.5) – двійкове k	(ν = 0.33) –трійкове k
Повні ЕКФЕ	1.51 (**max** 1.544)	1.574 (**max** 1.603)
Скручені ЕКФЕ	1.416 (**max** 1.544)	1.47 (**max** 1.603)

Порівняльний аналіз кількості операцій, які необхідно здійснити при експоненціювання точки на скрученій і на повній кривій Едвардса і кривій у формі Вейєрштрасса показав, що експоненціювання точки на кривих Едвардса швидше, ніж на кривих у формі Вейєрштрасса, більш ніж у 1,5 рази. Особливо ЕКФЕ виграють при трійковому представленні числа *k*.

Висновки до розділу 2

У розділі наведено загальні теоретичні властивості ЕКФЕ. Представлено універсальний модифікований закон додавання та подвоєння точок. На основі нової модифікації ЕКФЕ, введена арифметика для групових операцій з особливими точками цих кривих, надано аналіз точок малих порядків і формули, що пов'язують їх з іншими точками кривої. З застосуванням нової модифікації на базі аналізу параметрів кривої з використанням апарату кінцевих полів та алгебраїчної геометрії проведено теоретичне дослідження та аналіз ЕКФЕ над простими скінченними полями характеристики p > 3. Представлено нову повну класифікацію кривих в узагальненій формі Едвардса з використанням методом перебору квадратичності параметрів кривої. У порівнянні з існуючою класифікацією, запропонованою Bernstein D., Birkner P., Joye M., Lange T., Peters C. у роботі «Twisted Edwards Curves», за якою криві з різними властивостями належали до одного класу, у новій класифікації криві, в залежності від квадратичності параметрів a і d кривої у рівнянні (1), належать до трьох різних класів, що не перетинаються:

- повні криві Едвардса з умовою C1: $\chi(ad) = -1$;
- скручені криві Едвардса з умовами C2.1: $\chi(a) = \chi(d) = -1$;
- квадратичні криві Едвардса з умовами C2.2: $\chi(a) = \chi(d) = 1$.

де χ – квадратичний характер елементу поля.

Зроблено аналіз деяких властивостей кривих всіх 3-х класів і можливих значень порядків цих кривих. Описано алгоритм і дано результати розрахунку точної кількості кривих різних класів з мінімальним кофактором 4 порядку кривої при $p \equiv 1 mod 4$ и $p \equiv 3 mod 4$. Зроблено обґрунтований висновок, що існує приблизно 3/8 кривих Едвардса з мінімальним кофактором порядку кривої 4, що можуть бути використані у криптосистемах.

Розглянуто властивості кривих різних класів за новою класифікацією. Зроблено висновки щодо того, що повні і скручені ЕКФЕ можуть бути рекомендовані для використання в ЕСС, тому що не мають особливостей в підгрупі точок утворених генератором - усі точки мають скінченні координати, що спрощує процес програмування. Повні і скручені ЕКФЕ мають мінімальний кофактор 4 порядку кривої, мають високу швидкість експоненціювання точки, а на скручених ЕКФЕ генератор криптосистеми знаходиться у два рази швидше, ніж на повних. Квадратичні криві мають особливості в наявності чотирьох точок з нескінченними координатами, що ускладнює роботу з ними. Так само вони мають надмірну кількість точок через великий (не менше 8) мінімальний кофактор порядку кривої, що збільшує кількість операцій при пошуку генератора. Тому їх використовувати в ЕСС недоцільно, хіба що для теоретичного аналізу, так як квадратичні криві зі скрученими утворюють пару квадратичного крутіння.

Знайдено та доведено умови ізоморфізму ЕКФЕ і кривих у формі Вейєрштрасса, що дозволяє стверджувати, що ЕКФЕ мають аналогічні вимоги до забезпечення безпеки у відношенні рішення проблеми дискретного логарифма (DLP). Доведено теорема щодо визначення точного числа повних кривих Едвардса, ізоморфних кривим у формі Вейєрштрасса з ненульовими параметрами a и b. Наведено доказ двох тверджень щодо визначення порядків точок з використанням властивостей взаємозв'язку сімейств точок. На підставі цього розроблено та проілюстровано на прикладі новий метод реконструкції точок kP скалярного добутку ЕКФЕ, який у порівнянні з класичним методом

послідовного обчислення усіх точок, знижує трудомісткість обчислення у 8 разів та прискорює і спрощує програмування.

Проведено порівняльний аналіз складності групових операцій на кривих Вейерштрасса і на скручених і повних ЕКФЕ в проективних координатах. Запропоновано метод зменшення складності операцій шляхом використання мінімального значення параметра кривої, що дозволяє знехтувати складністю операції додавання і робить швидкість експоненціювання точки на скрученої кривої Едвардса рекордною. Описано метод зниження складності обчислень до нижніх меж $V_E = 10.67M$, $T_E = 5.67M$.

Порівняльний аналіз кількості операцій, які необхідно здійснити при експоненціювання точки на скрученій і на повній кривій Едвардса і кривій у формі Вейєрштрасса показав, що експоненціювання точки на кривих Едвардса швидше, ніж на кривих у формі Вейєрштрасса, більш ніж у 1,5 рази. Особливо ЕКФЕ виграють при трійковому представленні числа *k*.

Перелік використаних джерел до розділу 2

1. Бессалов А.В. Число ізоморфізмові и пар кручения кривых Эдвардса над простым полем. Радиотехника, вып. 167, 2011. С. 203-208.

2. Bessalov A.V., Tsygankova O.V. Interrelation of families of points of high order on the Edwards curve over a prime field. Problems of Information Transmission, 51(4), 2015. PP.391-397. http://link.springer.com/article/10.1134/S0032946015040080.

3. Бессалов А.В., Цыганкова О.В. Производительность групповых операций на скрученной кривой Эдвардса над простым полем. Радиотехника №181, 2015. – С.58-63.

4. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Теорія, практика, застосування: монографія. – Харків: Видавництво «Форт», 2012. – 870с.

5. Бессалов А.В., Цыганкова О.В. Взаимосвязь семейств точек больших порядков кривой Эдвардса над простым полем. Захист інформації –Том 17, №1, січень-березень 2015. –С.73-80.

6. Бессалов А.В., Цыганкова О.В. Число кривых в обобщенной форме Эдвардса с минимальным четным кофактором порядка кривой. Проблемы передачи информации, - Том 53, вып 1, 2017. С.101-111.

7. Цыганкова О.В., Цыганков Р.И. Анимация точек экспоненцирования кривой Эдвардса // тезиси докладів XV Всеукраїнської наукова-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики», 25-27 травня 2017р., м. Київ. Том II.– С. 114.

РОЗДІЛ 3 РОЗРОБКА МЕТОДІВ ЗНАХОДЖЕННЯ ТОЧКИ ПРОСТОГО ПОРЯДКУ КРИВИХ, ЩО НАЛЕЖАТЬ ДО КЛАСУ ПОВНИХ ТА СКРУЧЕНИХ ЕКФЕ

Вступ

Еліптичні криві у формі Едвардса (ЕКФЕ) над простим полем на сьогодні забезпечують найбільшу швидкість та є перспективними для використання в асиметричних криптосистемах. Найвища продуктивність, універсальність закону додавання, унікальна симетрія точок та наявність афінних координат нейтрального елемента групи – головні властивості ЕКФЕ, які були виявлені і обґрунтовані вже в першій роботі [1] фахівцями з криптографії. Важливим є також те, що ізоморфні криві завжди належать одному класу. Також в роботі [2] доведено, що продуктивність операції експоненціювання точки ЕКФЕ, порівняно з кривою у формі Вейєрштрасса, в середньому вище більш ніж в 1,5 рази. На підставі цього та згідно з доведеним ізоморфізмом ЕКФЕ та кривих Вейєрштрасса [1], ЕКФЕ можуть бути використані в задачах аналізу існуючих та створення нових алгоритмів і стандартів асиметричної криптографії.

У розділі розглянуто три варіанта створення алгоритмів пошуку генератора криптосистеми (базової точки) на ЕКФЕ над простим полем. У розділі 1 визначено властивості повних та скручених ЕКФЕ згідно з новою запропонованою класифікації ЕКФЕ [3]. Наведено властивості точок простого порядку та методи їх знаходження. Описано алгоритм знаходження базової точки на кривих Вейєрштрасса та розроблено та описано нові алгоритми знаходження базової точки для побудови криптосистеми на повних та скручених ЕКФЕ. Зроблено порівняльний аналіз швидкодії алгоритмів на ЕКФЕ та на кривих, що використовуються в стандартах цифрового підпису (ЦП).

3.1 Алгоритми пошуку базової точки на повних та скручених ЕКФЕ

Важливою властивістю повних та скручених ЕКФЕ є те, що при $p \equiv 1 mod 4$ вони мають мінімальний парний кофактор порядку кривої 4: $N_E = 4n$ де $n \in \mathbb{P}$. Циклічна підгрупа скручених ЕКФЕ простого порядку n має такі ж самі корисні

для криптографічних застосувань і стандартизації властивості, що і повні ЕКФЕ [3]. В алгоритмі ЦП важливим кроком є знаходження генератора криптосистеми - тобто базової точки простого порядку *n*. Для створення алгоритму пошуку базової точки для побудови криптосистеми на повних та скручених кривих було розглянуто декілька варіантів знаходження точок простого порядку.

Один з алгоритмів знаходження базової точки на повних ЕКФЕ було розроблено на запропонованому методі знаходження точки максимального порядку $4n$ [5], розробленого на підставі 3-х теорем щодо властивостей точок повної ЕКФЕ:

Теорема 3.1 Для будь-якої точки (*x*,*y*) повної кривої Едвардса, що не належить колу радіуса 1, існують 2 точки ділення на 2 $\{P, P+D\}$ тоді і тільки тоді, коли $\chi(1-y^2)=1$.

Доведення

Скористуємося методом заміни змінної. Якщо взяти лише точки, порядки яких більше 4, та у формулах зробимо заміну

$$X = x_1^2, Y = y_1^2, Z = Y/X, V = XY, X, Y \neq 0.$$

Зробимо заміну у знаменнику (2.2) на $(X+Y)$ та $(2-X-Y)$ відповідно. Згідно з (2.1) та (2.3) для однієї точки P кривої $ordP > 4$ справедливі вирази:

$$Z^2 - 2x^{-1}Z + 1 = 0,$$

$$dV^2 - 2x^{-1}V + 1 = 0, x \neq 0,1. \qquad (3.1)$$

Дискримінанти

$$\Delta_1 = 4x^{-2}(1-x^2),$$

$$\Delta_2 = 4x^{-2}(1-dx^2), \qquad (3.2)$$

та розв'язок

$$Z_{1,2} = x^{-1}\left(1 \pm \sqrt{1-x^2}\right),$$

$$V_{1,2} = (xd)^{-1}\left(1 \pm \sqrt{1-dx^2}\right). \qquad (3.3)$$

Необхідність. Подвоєння будь якої точки P з ненульовими координатами згідно з законом (2.2) породжує єдину точку $2P = (x, y)$, та координати точок P і $2P$ є розв'язок двох рівнянь (3.1) у полі $\boldsymbol{F}_p$. Необхідною умовою існування розв'язку

першого з рівнянь (3.1), як слідує з (3.2), є те, що елемент поля $\chi(1-x^2)=1$. При виконанні цієї умови окрім точки P, для якої $2P=(x,y)$, існує ще одна точка $P^*=P+D=(-x_1,-y_1)$, для якої $2P^*=2P+2D=(x,y)$, так як $2D=0$. При $\chi(1-x^2)=-1$ рівняння (3.1) розв'язків в полі немає. Необхідність умови теореми 3.1 доведено.

Достатність. Для будь якої точки кривої (2.1), у якої $ordP>4$, для якої має місце розв'язок (2.3), справедливо дві тотожності (3.1). Достатньо, щоб один з дискримінантів (3.2) був квадратичним лишком, тоді другий дискримінант теж буде квадратичним лишком. Нехай точка$P=(x,y)$ належить кривій (2.1) де $a=1$. Тоді рівняння $x^2+y^2=1+dx^2y^2$ можна записати як $(1-y^2)=x^2(1-dy^2)$. Звідси вочевидь випливає, що для будь-якої точки (x,y) кривої вирази $(1-y^2)$ та $(1-dy^2)$ є обидва квадратичними лишками або нелишками. У першому випадку існує дві точки ділення на 2, а в іншому випадку – не існує. Теорему 3.1 доведено [6].

Теорема 3.2 Необхідною і достатньою умовою існування 4-х точок 8-го порядку повної кривої Едвардса є $\chi(1-d)=1$.

Доведення

Необхідність. Нехай $Ord(P)=8$, тоді $2P=F$. Відповідно з формулою (2.2) для координат $P=(x,y)$ маємо:

$$\frac{2xy}{(1+dx^2y^2)}=1,\quad \frac{y^2-x^2}{(1-dx^2y^2)}=0.$$

Звідси $y^2=x^2 \implies dx^4-2x^2+1=0 \implies x^2=1\pm\sqrt{1-d}$.

Тобто умова $\chi(1-d)=1$ теореми є необхідною умовою існування координат $x=\pm y$.

Достатність. Доведемо, що умова теореми завжди породжує рівно 4 точки 8-го порядку. Так як додаток $\left(1+\sqrt{1-d}\right)\left(1-\sqrt{1-d}\right)=d,$ то одне з значень у рівності $x^2=1\pm\sqrt{1-d}$ є квадратичним лишком, а друге – нелишком. Якщо вибирати двійковим квадрат з цієї альтернативи $(1+(-1)^{\kappa}\sqrt{1-d})$, $\kappa\in\{0,1\}$, отримуємо 4 точки $(\pm x,\pm y)$ 8-го порядку. Теорему 3.2 доведено [8].

Теорема 3.3 Для будь-якої точки (x, y) повної кривої Едвардса, що не належить колу радіуса 1, справедлива рівність $\chi(1-x^2)\cdot\chi(1-y^2)=\chi(1-d)$.

Доведення

Для точки (x, y) з урахуванням (1) де $a=1$ запишемо додаток

$$(1-y^2)(1-x^2)=1+x^2y^2-x^2-y^2=y^2-dy^2=(1-d)x^2y^2.$$

Тоді з останнього співвідношення випливає, що додаток $(1-y^2)(1-x^2)$ є квадратичним нелишком при $\chi(1-d)=-1$, та навпаки, що і доводить твердження теореми 3 [6].

Метод знаходження точки максимального порядку полягає у тестуванні значення символу Лежандра або квадратичного характеру виразу $(1-y^2)$. Якщо виконується умова $\chi(1-d)=-1$, то відповідно до теореми 2, крива не має точок 8 порядку і порядок кривої $N_E = 4n$, де $n \in$ P. Таким чином якщо $\chi(1-y^2)=-1$, то $\chi(1-x^2)=1$ і навпаки, що дає можливість знайти точку максимального порядку одним тестуванням характеру квадратичності $(1-y^2)$ координати випадкової точки кривої. Практично $1/2$ випадкових точок кривої мають порядок $4n$, $1/4$ – порядок $2n$ та $1/4$ – порядок n [4].

На базі методу знаходження точки максимального порядку та властивостей точок ЕКФЕ щодо подвоєння точки максимального порядку, розроблено метод знаходження точки простого порядку, який використано в трьох детермінованих алгоритмах пошуку генератора криптосистеми. Алгоритм 3.1 (рис. 3.1) обчислення генератора криптосистеми, тобто точки простого порядку n на повній ЕКФЕ.

***Алгоритм* 3.1**:

умови: ЕКФЕ має вигляд (1), де $\chi(ad)=-1$, $N_E=4n, n\in\mathbb{P}, p\equiv 1 mod 4$.

1. знаходиться випадкова координата x точки $P=(x,y)$;

2. якщо $x=0,$ або $\pm 1,$ або $\pm\frac{1}{\sqrt{d}}$,то перейти до кроку1;

3. обчислюється $z=(1-x^2)(1-dx^2)^{-1} mod p$;

4. якщо $\chi(z) \neq 1$, то перейти до кроку 1;

5. обчислюється $y = \sqrt{z} mod p$;

6. якщо $\chi(1 - y^2) \neq 1$, то $x \leftrightarrow y$; $P \leftarrow (y, x)$;

7. обчислюється $G = 2P$;

вихід: точка $G = (x_G, y_G)$, така, що Ord(G) = n.

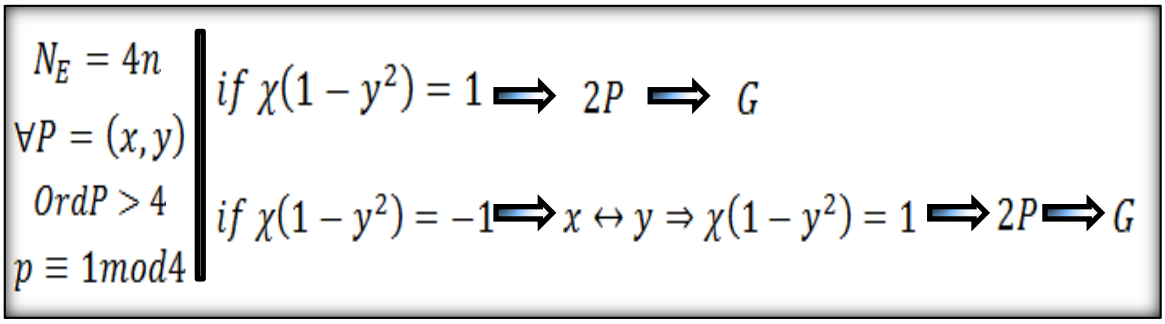


Рисунок 3.1 – Алгоритм 1 находження базової точки на повних ЕКФЕ

Згідно з властивостями порядків точок повної ЕКФЕ над полями F_p, де $p \equiv 1 mod 4$, подвоєння точки максимального порядку $4n$ створює точку, порядок якої дорівнює $2n$. Подвоєння точки порядку $2n$ створює точку простого порядку n. На підставі цієї властивості порядків точок повної ЕКФЕ розроблено Алгоритм 2 (рис. 3.2) знаходження точки простого порядку.

***Алгоритм* 3.2**:

умови: ЕКФЕ має вигляд за формулою (1) де $\chi(ad) = -1, N_E = 4n, n \in \mathbb{P}$, $p \equiv 1 mod 4$.

1. знаходиться випадкова координата x точки $P = (x, y)$;

2. якщо $x = 0, \text{або } \pm 1, \text{або } \pm \frac{1}{\sqrt{d}}$, то перейти до кроку1;

3. обчислюється$z = (1 - x^2)(1 - dx^2)^{-1} mod p$;

4. якщо $\chi(z) \neq 1$, то перейти до кроку 1;

5. обчислюється $y = \sqrt{z} mod p$;

6. обчислюється $G = 4P$;

вихід: точка $G = (x_G, y_G)$, така, що Ord(G) = n.

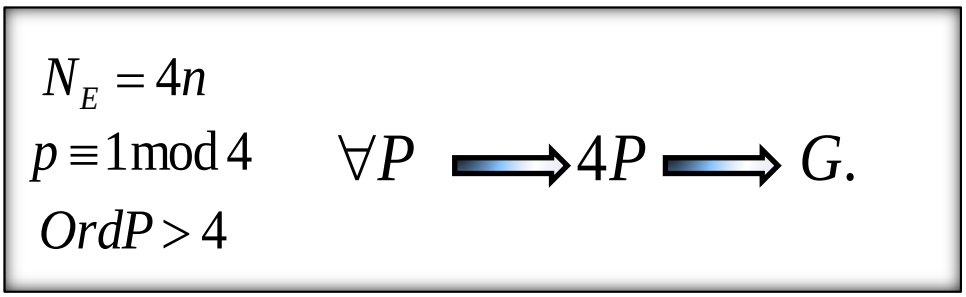


Рисунок 3.2 – Алгоритм 2 знаходження базової точки на повних ЕКФЕ

Для скрученої ЕКФЕ знаходження точки простого порядку прискорюється удвічі завдяки одному подвоєнню випадкової точки. На підставі цього розроблено найшвидший Алгоритм 3.3 (рис. 3.3).

***Алгоритм* 3.3**:

умови: ЕКФЕ має вигляд за формулою (1) де $\chi(a) = \chi(d) = -1$, $N_E = 4n, n \in \mathbb{P}$, $p \equiv 1 mod 4$.

1. знаходиться випадкова координата x точки $P = (x, y)$;
2. якщо $x = 0, \text{або } \pm 1, \text{або } \pm \frac{1}{\sqrt{d}}$, то перейти до кроку1;
3. обчислюється $z = (1 - x^2)(1 - dx^2)^{-1} mod p$;
4. якщо $\chi(z) \neq 1$, то перейти до кроку 1;
5. обчислюється $y = \sqrt{z} mod p$;
6. обчислюється $G = 2P$;

вихід: точка $G = (x_G, y_G)$, така, що Ord(G) = n.

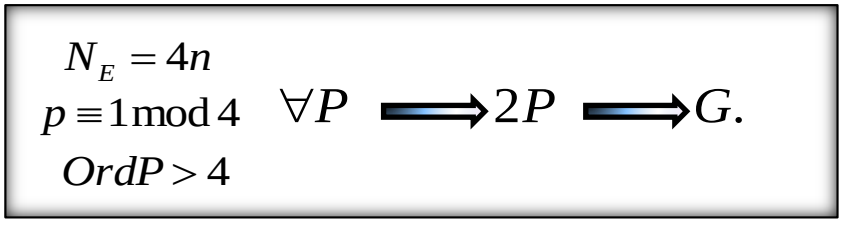


Рисунок 3.3 – Алгоритм 3 знаходження базової точки на скручених ЕКФЕ

3.2 Порівняльний аналіз швидкодії алгоритмів знаходження базової точки для побудови криптосистеми на ЕКФЕ та кривих у формі Вейєрштрасса

Алгоритми знаходження базової точки на повних та скручених ЕКФЕ виглядають значно простішими та швидкими у порівняно зі стандартним алгоритмом на канонічній кривій. Необхідно провести порівняльний аналіз швидкодії цих алгоритмів.

Стандартний алгоритм ЦП на еліптичних кривих:

1. знаходиться випадкова точка $P = (x, y)$;
2. обчислюється скалярний добуток nP;
3. якщо $(nP) \neq \mathbf{O}$, то перейти до кроку 1;
4. якщо $(nP) = \mathbf{O}$, то $P = G$;

вихід: точка $G = (x_G, y_G)$.

Знаходження кількості операцій, які потрібно виконати при пошуку точки простого порядку на кривих Вейєрштрасса в стандартному алгоритмі [7]:

- пошук точки, стандартним методом, що належить кривій, потребує 8 кроків до успіху;
- обчислення скалярного добутку nP в проективних координатах потребує $\log(n)$ подвоєння. Всього $5.67M\log(n)$ операцій. У середньому $0.5\log(n)$ додавання точок;
- $0.5 \cdot 11.17M\log(n) = 5.58M \cdot \log(n)$, де M – кількість множень у полі;
- загальне число операцій у полі з урахуванням 4-х кроків (в середньому) до успішного результату:

$$S = 8 \cdot 4 \cdot (5.67 + 5.58)M \cdot \log(n) = 360M \cdot \log(n).$$

Знаходження кількості операцій в запропонованих алгоритмах 1, 2 та 3 виконувався таким же чином [6, 7].

Розрахунок кількості операцій, які потрібно виконати при пошуку точки простого порядку в Алгоритмі 1:

- пошук точки. Невдача: $\forall$ точка, якщо $x = 0, \pm 1, \pm\frac{1}{\sqrt{\mathrm{d}}}$; та $\forall\ \chi(z) \neq 1$.

Якщо умови x виконуються $\Longrightarrow$ можна вважати, що z – виконуються. $\Longrightarrow$ $p(\chi(z) \neq 1) = \frac{1}{2}$. Тому, імовірність успіху $\geq 1 - \frac{1}{2} - \frac{4}{n} \approx \frac{1}{2}$ $\Longrightarrow$ середня кількість до успіху дорівнює 2 крокам.

- обчислення $(1 - y^2)$ потребує $0{,}67M$ операцій;
- обчислення символу Лежандра $\chi(1 - y^2)$ потребує $M\log(n)$;
- одне подвоєння точки потребує $0{,}67M$ операцій;
- сумарна кількість операцій у полі:

$$S_1 = 2 \cdot (5.67 + 0.68 + \log(n)) \cdot M == 2 \cdot (6.34 + \log(n))M.$$

Розрахунок кількості операцій, які потрібно виконати при пошуку точки простого порядку в Алгоритмі 3.2:

- пошук точки. Середня кількість до успіху дорівнює 2 крокам. (див. Алгоритм 3.1);
- обчислення $G = 4P$ потребує два подвоєння;
- сумарна кількість операцій у полі:

$$S_2 = 2 \cdot 2 \cdot 5.67M = 22.68M.$$

Розрахунок кількості операцій, які потрібно виконати при пошуку точки простого порядку в Алгоритмі 3.3:

- Пошук точки. Середня кількість до успіху дорівнює 2 крокам. (див. Алгоритм 3.1);
- Обчислення $G = 2P$ потребує одне подвоєння;
- Сумарна кількість операцій у полі:

$$S_3 = 11{,}34M.$$

Усі значення кількості операцій у групі, які потрібно виконати при пошуку точки простого порядку в алгоритмах пошуку базової точки, записано у таблиці 3.1.

Таблиця 3.1 - Кількості операцій при пошуку генератора криптосистеми

Алгоритми	Кількість операцій у полі, де M– кількість множень у полі
Стандартний алгоритм	$S = 360M \cdot \log(n)$
Алгоритм 1	$S_1 = (12{,}68 + 2\log(n))M$
Алгоритм 2	$S_2 = 22{,}68M$
Алгоритм 3	$S_3 = 11{,}34M$

На підставі отриманих результатів можна зробити порівняльний аналіз швидкодії та отримати значення виграшу γ для усіх запропонованих алгоритмів.

$$\gamma_1 = \frac{S}{S_1} = \frac{360M \cdot \log(n)}{2 \cdot (6.34 + \log(n))M} \approx 180$$

$$\gamma_2 = \frac{S}{S_2} = \frac{360M \cdot \log(n)}{22{,}68M} \approx 16\log(n)$$

$$\gamma_3 = \frac{S}{S_3} = \frac{360M \cdot \log(n)}{11{,}34M} \approx 32\log(n)$$

За розрахунком значення виграшу нових алгоритмів порівняно зі стандартним алгоритмом, було отримано результати:

- виграш у швидкодії Алгоритму 1 порівняно зі стандартним алгоритмом у $\gamma_1 = \frac{S}{S_1} \approx 180$ разів;
- виграш у швидкодії Алгоритму 2 порівняно зі стандартним алгоритмом у $\gamma_2 = \frac{S}{S_2} \approx 16\log(n)$ разів.
- виграш у швидкодії Алгоритму 3 порівняно зі стандартним алгоритмом у $\gamma_2 = \frac{S}{S_3} \approx 32\log(n)$ разів.

Результати обчислень дають змогу зробити обґрунтовані висновки, що знаходження генератора на ЕКФЕ із застосуванням запропонованих алгоритмів порівняно зі стандартним алгоритмом істотно більш швидше і відповідно ефективніше.

Висновки до розділу 3

У **розділі** досліджено властивостей ЕКФЕ над простими полями, що належать до класу повних та скручених кривих за новою класифікацією, та знайдено методи знаходження точок заданого порядку, що надало змогу рекомендувати їх використання в асиметричних криптосистемах. Проведено аналіз циклічних ЕКФЕ, який дозволив виявити низку нових властивостей повної ЕКФЕ над простим полем. Сформульовано та доведено 3 теореми про властивості точок повної ЕКФЕ. На підставі доведення цих теорем запропоновано новий метод визначення точки максимального порядку, який використано у розробці нового методу знаходження базової точки повної ЕКФЕ. Виконано порівняльний аналіз деяких властивостей скручених кривих Едвардса з повними та виявлено, що скручені ЕКФЕ мають головну відмінність – нециклічну структуру групи точок 2-го порядку і наявність серед них двох особливих точок (з діленням на 0 y-координати), що робить їх застосування в деяких задачах еліптичної криптографії проблематичним.

Знайдено та обґрунтовано умови існування точок 2, 4 і 8 порядків, при виконанні яких скручені ЕКФЕ мають порядок $N_E = 4n$ (де n – просте число) та відсутність особливих точок у підгрупі точок простого порядку n, що відповідає вимогам щодо кривих, які можуть бути застосовані для побудови криптоалгоритмів. Крім того, у процесі досліджень було виявлено, що скручені ЕКФЕ при $N_E = 4n$ мають точки максимального порядку $2n$, що прискорює пошук точки простого порядку у 2 рази. Така специфічна особливість надала змогу створити новий детермінований алгоритм визначення пошуку генератора криптосистеми на скручених ЕКФЕ.

Вперше отримані необхідні і достатні умови подільності на 2 точок скрученої кривої Едвардса на підставі яких розроблено нові методи знаходження порядку точок скрученої кривої, з застосуванням яких розроблено нові алгоритми пошуку генератора криптосистеми.

Зроблено аналіз кількості операцій у полі у групових операціях додавання і подвоєння точок повних та скручених ЕКФЕ при знаходженні точок простого порядку – генератора криптосистеми. За результатами порівняння аналізу оцінок групових операцій визначено, що у загальному випадку найменших обчислювальних витрат вимагають операції на повних ЕКФЕ. Особливо повні ЕКФЕ виграють при подвоєнні, яке обходиться без операції множення на параметр кривої.

Запропоновано метод досягнення мінімальної складності операцій, за наслідком використання якого з'явилася можливість зменшити складність додавання у групі точок через зневагу параметрами як малими числами.

З використанням запропонованих методів знаходження точок простого порядку розроблено три алгоритми пошуку генератора криптосистеми на повних та скручених ЕКФЕ

У розділі розв'язано актуальну науково-практичну задачу дослідження властивостей еліптичних кривих у формі Едвардса, придатних для використання в алгоритмах асиметричних криптосистем, зокрема, в алгоритмах цифрового підпису, які дозволяють підвищити швидкодію експоненціювання точки в цих криптосистемах. Проведені дослідження дозволили запропонувати три нових алгоритми пошуку генератора криптосистеми для побудови криптосистеми на повних та скручених ЕКФЕ, які швидше стандартного алгоритму ЦП на кривих у формі Вейєрштрасса у 180, $16\log(n)$ та $32\log(n)$ (де $n \in \mathbb{P}$) разів відповідно. Результати роботи можуть бути використані в задачах аналізу існуючих та створення нових алгоритмів і стандартів асиметричної криптографії.

Перелік використаних джерел для розділу 3

1. Bernstein Daniel J., Lange Tanja. Faster addition and doubling on elliptic curves. IST Programme under Contract IST–2002–507932 ECRYPT, 2007, PP. 1-20.
2. Бессалов А. В., Цыганкова О. В. Производительность групповых операций на скрученной кривой Эдвардса над простым полем. // Радиотехника №181, 2015. С.58-63.
3. Бессалов А. В., Цыганкова О. В. Классификация кривих в форме Эдвардса над простым полем. // Прикладная радиоелектроника, Том 14 № 3, 2015. С.197-203.
4. Bessalov A. V., Tsygankova O. V. New properties of the Edwards form elliptic curveover a primefield // Telecommunications and Radio Engineering (English translation of Elektrosvyaz and Radiotekhnika) №180 2015. pp.137-143.
5. Bessalov A. V., Tsygankova O. V. Interrelation of families of points of highorderon the Edwards curve over a primefield // English translation of Problems of Informati on Transmission, 2015, Vol. 51, № 4, pp. 391-397. sci-hub.tw/10.1134/S0032946015040080
6. Бессалов А. В., Цыганкова О. В. Метод определения точек максимального порядка на кривой Эдвардса. // Спеціальні телекомунікаційні системи та захист інформації. Збірник наукових праць, випуск 2(26), 2014. С.18-21.
7. Bernstein Daniel J.,Birkner Peter, JoyeMarc, Lange Tanja, Peters Christiane. Twisted Edwards Curves.//IST Programme under Contract IST–2002–507932 ECRYPT, and in part by the National Science Foundation under grant ITR–0716498, 2008, PP. 1-17.
8. Бессалов А. В. Эллиптические кривые в форме Эдвардса и криптография: монографія // изд-во «Политехника», КПИ им. Игоря Сикорского, Киев. 2017. – 272с.

РОЗДІЛ 4 ПАРАМЕТРИ СТІЙКИХ МАКСИМАЛЬНО ШВИДКИХ ЕКФЕ

У розділі 4 поставлено і виконано задачу пошуку кривих Едвардса з майже простим значенням порядку $4n$ над великими простими полями. Наведено алгоритм пошуку крипостійкої повної кривої Едвардса на базі ізоморфної кривої в формі Вейерштрасса.

У розділі 4.1 і ДОДАТКУ А наводяться табульовані результати обчислень загальносистемних параметрів криптостійких повних кривих Едвардса, придатних для стандартизації.

У розділі 4.2 і ДОДАТКУ Б наводяться табульовані результати розрахунків загальносистемних параметрів криптостійкі скручених кривих Едвардса над простим полем у всьому діапазоні стандартних значень модуля поля.

4.1 Обчислення загальносистемних параметрів криптостійкі повних кривих Едвардса

Цільовим завданням дослідження властивостей кривих в формі Едвардса є впровадження ефективної технології, в проекти нових стандартів еліптичної криптографії. Існуючі стандарти [1] рекомендують, як правило, набір кривих над кінцевими полями в широкому діапазоні вимог по їх кріптостійкості. Наприклад, перший з таких стандартів - національний стандарт США FIPS-186-2-2000 [2] - рекомендує 5 кривих в формі Вейерштрасса над простими полями з довжинами модулів від 192 до 521 біта. В даному розділі ми взяли за основу ті ж поля і вирішили задачу обчислення загальносистемних параметрів криптостійких повних кривих Едвардса порядку 4n с простим порядком n точки G - генератора криптосистеми. Ці результати опубліковані в роботі [3] і обговорювалися на конференціях [4, 6].

Пошук кривих Едвардса, прийнятних для криптографії, є нетривіальне завдання. Ключовим моментом в ній є розрахунок порядку кривої, заданої над кінцевим полем. У даній роботі поставлена задача пошуку повних кривих

Едвардса з майже простим значенням порядку $4n$ над великими простими полями. У першій частині розділу обговорюємо проблему визначення порядку кривої в формі Едвардса і коротко описуємо можливі шляхи і алгоритм її вирішення. У другій частині розділу наводимо методи розрахунків і наші результати обчислень загальносистемних параметрів 40 кривих Едвардса над простими полями Fp з модулями p довжиною 192, 224, 256 і 384 біт [3]. Порядок $4n$ запропонованих кривих містить простий співмножник n, близький за величиною до величини відповідного поля. Таким чином, знайдені криві задовольняють сучасним вимогам до порядку генератора криптосистеми і з успіхом можуть застосовуватися на практиці і в проектованих криптосистемах.

В роботі [7] доведено, що для будь-якої кривої, записаної у формі (2.1), знайдеться ізоморфна еліптична крива в канонічній формі над полем Fp. Однак, в відомих стандартах шифрування на еліптичних кривих [8] не міститься кривих над простими полями з кофактором порядку, рівним 4. Це не дозволяє перетворити рекомендовані сучасними стандартами криві безпосередньо в форму (2.1). У зв'язку з цим для криптографічних додатків слід провести пошук кривих Едвардса над простими полями з прийнятним значенням порядку $4n$.

4.1.1 Алгоритм пошуку крипостійкої повної кривої Едвардса на базі ізоморфної кривої в формі Вейерштрасса

У розділах 1.5 і 1.6 були приведені алгоритми пошуку крипостійкість повної кривої Едвардса введенням нового параметра c в рівняння канонічної кривої. Тут ми інтегруємо ці алгоритми в більш загальний алгоритм, який використовує прямі формули ізоморфного перетворення кривої в формі Вейерштрасса в криву Едвардса. Як нам вже відомо з розділу 1, для кожної кривої (4.1) в формі Едвардса E знайдеться ізоморфна їй крива у формі Вейерштрасса W виду

$$W: \quad v^2 = u^3 + au + b. \qquad (4.1)$$

Відповідний ізоморфізм між точками кривих E і W задається раціональними функціями [9]:

$$u = \frac{(5-d)+(1-5d)y}{12(1-y)}, \quad v = \frac{(1-d)+(1+y)}{4x(1-y)}, (y-1) \neq 0. \qquad (4.2)$$

Хоча вони складніше формул (1.20) для кривих в формі Монтгомері, вони задають прямий ізоморфізм ($W \to E$) без використання проміжної форми Монтгомері ($W \to M \to E$).

Чотири точки перетину з осями координат перетворюються в такий спосіб:$(x, y) = (0, 1) \to (u, v) = O$,

$$(x, y) = (0, -1) \to (u, v) = \left(\frac{1+d}{6}, 0\right) \text{ при } x = 0.$$

$$(x, y) = (\pm 1, 0) \to (u, v) = \left(\frac{5-d}{12}, \pm\frac{1-d}{4}\right) \text{ при y= } \pm 1$$

Коефіцієнти кривої *W* виражаються через параметр кривої *E* наступним [9]:

$$a = -\frac{(1+14d+d^2)}{48}, b = -\frac{(1-33d-33d^2+d^3)}{864}. \qquad (4.3)$$

Для зворотного перетворення справедливо:

$$x = \frac{6u-(1+d)}{6v}, \qquad y = \frac{12u+d-5}{12u+1-5d},$$

При $6v(12u + 1 - 5d) \neq 0$,

$$(u, v) = \left(\frac{1+d}{6}, 0\right) \to (x, y) = (0, -1), \qquad \text{при } v = 0,$$

$$(u, v) = O \to (x, y) = (0, 1). \qquad (4.4)$$

Одним із способів розрахунку порядку кривої Едвардса є адаптація відповідних методів знаходження порядку канонічних еліптичних кривих (таких як алгоритми СКУФ, SEA, Satoh). Використовуючи співвідношення (4.2) - (4.4), для кривих в формі Едвардса визначається послідовність поліномів розподілу [9], за допомогою яких методом SEA може бути обчислений порядок розглянутої кривої Едвардса. З іншого боку, підрахувати порядок кривої Едвардса можна за допомогою ізоморфного переходу до канонічної формі з подальшим перебуванням порядку кривої за відомими алгоритмами.

Другий сценарій був використаний для пошуку кривих над простими полями, наведених [10]. Вибравши довільно параметр d ≠ A ^ 2 в полі *Fp* і, використовуючи формули (4.3), отримаємо ізоморфну еліптичну криву в формі Вейерштрасса. Зауважимо, що при заданому обмеженні на параметр d кривої,

кубика правій частині рівняння (4.1) буде мати єдиний корінь c, і буде виконуватися також умова (ii) існування двох точок 4-го порядку теореми 3.6. [10] Порядок N_E ЕКФЕ вважаємо прийнятним, якщо число $n = N_E/4$ просте, що лежить приблизно в межах 180 - 600 біт. Така крива може бути рекомендована до застосування в криптопротоколів.

Для побудови криптографічного системи на отриманої ЕКФЕ необхідно визначити генеруючу точку G порядку n. Ставлячи довільно координату x і обчислюючи з рівняння кривої (3.1) значення у отримаємо довільну точку Q ЕКФЕ. Або $x \neq 0$ и $x \neq \pm 1$ (ймовірність цієї події дуже мала), порядок точки Q може дорівнювати $n = N_E/4$, $2n$ или $4n = N_E$. Тоді генератором криптосистеми буде точка Q, $2Q$ або $4Q$ відповідно. В розділі 3.5 запропоновано метод знаходження генератора одного подвоєння точки Q.

4.1.2 Загальносистемні параметри криптостійкі повних кривих Едвардса

В даному розділі ми розглядаємо прості поля с модулями

$p_{192} = 2^{192} - 2^{64} - 1,$

$p_{224} = 2^{224} - 2^{96} + 1,$

$p_{256} = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1,$

$p_{384} = 2^{384} - 2^{128} - 2^{96} + 2^{32} - 1,$

рекомендовані стандартом FIPS - 186 - 2 - 2000 [2], і наводимо перелік кривих в формі Едвардса майже простого порядку $N_E = 4n$ (n – просте) над кожним з полів. Дані наведені в таблицях 5.1 - 5.8 ДАДАТКУ А. Поряд з цим, в таблицях також містяться загальносистемні параметри для реалізації шифрування за допомогою кривої Едвардса, а саме, порядок $n = N_E/4$ і координати (x_G, y_G) генератора G криптосистеми для кожної кривої.

У кожній з наведених в ДОДАТКАХ А таблиць міститься по 10 кривих Едвардса над відповідним полем з параметрами d різної бітової довжини. Порядок кривих порівняємо по довжині з довжиною розглянутого поля.

Розрахунки проводилися за допомогою прикладних програм, заснованих на використанні функцій бібліотеки MIRACL.

На сьогоднішній день відкритої залишається завдання адаптації алгоритмів обчислення порядку кривої для кривих в формі Едвардса. Широко використовуються для цього завдання методи SEA та Satoh працюють з кривими в формі Вейерштрасса над великими простими полями і розширеними полями характеристики 2. Однак прийнятні повні ЕКФЕ над простими полями можна отримати за допомогою трансформації кривої Едвардса в ізоморфну криву у формі Вейерштрасса з подальшим визначенням порядку кривої в формі Вейерштрасса.

Таким способом в даній роботі отримано загальносистемні параметри 39 повних ЕКФЕ придатних для використанні у полях простого порядку, що рекомендовані стандартами $p_{192}, p_{224}, p_{256}, p_{384}$. Порядок кривих, наведених в розділі 3 [10], має мінімально можливий кофактор, рівний 4, і простий співмножник n, який можна порівняти за довжиною з довжиною відповідного поля. Це робить можливим застосування отриманих кривих в асиметричних криптосистемах, а загальносистемні параметри криптостійких кривих Едвардса можуть бути рекомендовані для стандартизації. Завдяки виграшу у швидкодії (в середньому в 1.5 - 1.6 рази, див. розділ 3.2) і зручності програмування криптосистем на ЕКФЕ алгоритми, що розроблено на ЕКФЕ стають ефективною альтернативою канонічної формі еліптичних кривих.

4.2 Результати розрахунку загальносистемних параметрів криптостійкі скручених кривих Едвардса з мінімальною складністю

В даному розділі розглядаються прості поля с модулями довжиною 192, 224, 256, 384 і 521 біт, які рекомендуються стандартом FIPS-186-4-2013, і наводяться перелік параметрів повних та скручених кривих Едвардса майже простого порядку $N_E = 4n\,(n$ – просте) над кожним з полів. Результати розрахунків загальносистемних параметрів кривих в шістнадцятковій системі числення

зведені в таблицях 1-5 Додатків А та Б. Тут модулі довжини L позначені як p_L. Модулі полів $p \equiv 5 mod 8$ вибиралися як прості числа, при яких елемент 2 є квадратичний не лишок і з малою двійковою вагою Хеммінга 3..5. Для таких полів значення параметру $a = 2$ фіксується як мінімальний не лишок, після чого послідовним нарощуванням визначалося мінімальне значення параметра d, при якому співмножник n порядку кривої - просте число. Такий алгоритм більш трудомісткий, ніж в попередній роботі [5], але забезпечує реальну мінімізацію складності обчислень і, відповідно, максимальну швидкість експоненціювання точки. Зокрема, значення $a = 2$ відповідає одному додаванню в поле, а ця операція зазвичай оцінюється як безкоштовна і ігнорується при оцінці складності обчислень. Для кожної кривої наведені значення p, значення параметрів a и d, порядки $n = N_E/4$ генератора G криптосистеми і його координати $G = (x_G, y_G)$.

Зауважимо, що параметр a = 2 є квадратичним не лишком лише при $p = \pm 3 mod 8$. Це означає, що двійкове представлення числа p закінчується трьома молодшими розрядами $101 = 5_{10}$ або $011 = 3_{10}$, а все більш старші розряди дають $0 mod 8$. В роботі [5] при випадковому пошуку простих чисел з малою вагою лише одне значення $p = 2^{255} + 2^{38} + 2^2 +$ в таблиці 5 відповідає цій умові (при цьому $a = 2$), тому практично всі криві в [5] мають мінімальний параметр $a = 3 \ldots 5$. Разом з тим в [5] варіювалися значення характеристики поля p для кожної кривої, тому для деяких модулів параметри d в таблицях цієї роботи мають менші значення.

Перевірка чисел p і n на простоту проводилася за допомогою тестів Міллера-Рабіна і Лукаса-Лемера, реалізованих в мовах програмування C #, Java і в системі Wolfram Mathematica.

Обчислення символів Лежандра для знаходження відповідного параметра d виконувалось за допомогою бібліотечних функцій мови Java і системи Wolfram Mathematica.

Порядки еліптичних кривих розраховувалися за алгоритмом SEA (Schoof-Elkies -Atkin), реалізованому в бібліотеці PARI / GP.

Точки G як генератори криптосистеми були знайдені подвоєнням випадкової точки, що задовольняє рівняння (2.1), з використанням системи Wolfram Mathematica і мови Java. Одного подвоєння досить, так як на

нециклічній скручені криві порядку $4n$ максимальний порядок точки дорівнює $2n$.

У кожній з наведених у Додатку Б таблиць містяться параметри 25 скручених кривих Едвардса з мінімальним значенням параметра $a = 2$, Далі параметр d підбирався як найменше з значень, при якому порядок криво $4n$ є майже просте число (n просте). Порядок кривих по довжині порівняно з довжиною поля.

Порівняємо ці результати з розрахованими параметрами кривих в [5]. Для модулів довжини 192 і 521 кращі параметри (d = 75 і d = 77 відповідно) отримані в даній роботі. Однак для інших трьох модулів в попередній роботі [5] при a = 3 найменші значення d виявилися меншими, ніж в таблицях 1 - 5: d = 38 при L = 224, d = 108 при L = 256, d = 236 при L = 384. Це зрозуміло, тому що варіювання значенням p дає додатковий резерв при пошуку кривої. Тому при виборі ЕКФЕ, що підходить за параметрами поряд зі справжньою роботою слід звертатися також до результатів, отриманих в [5].

На закінчення відзначимо, що запропоновані для стандартизації та імплементації скручені ЕКФЕ мають найвищу швидкість експоненціювання точки. Всі розраховані криві поряд з мінімальним значенням параметра $a = 2$ мають найчастіше 2-х або 3-х розрядне десяткове значення другого параметра d, що практично дозволяє знехтувати складністю операцій $1U$ і $2U$ для скручених кривих. Оцінки складності складання точок $V_E = 10M + 1S + 2U$ і подвоєння точки $T_E = 3M + 4S + 1U$ досягають в нашому випадку низьких меж $V_E = 10M + 1S = \frac{32}{3}M$, $T_E = 3M + 4S = \frac{17}{3}M$, якщо прийняти $S = \frac{2}{3}M$ [2]. Подібні результати для повної кривої Едвардса [3] програють результатами цієї роботи, так як в них параметри d порівнянні з розмірами модулів, при цьому

$1U \cong 1M$. Крім того, тут, на відміну від [3], знайдені криві для модулів поля p_{521} з найвищим стандартним рівнем стійкості.

Висновки до розділу 4

У розділі 4 дослідження дисертаційної роботи отримали подальшого розвитку у застосуванні розроблених алгоритмів пошуку генератора криптосистеми на повних та скручених ЕКФЕ. З застосуванням Алгоритму 2, який базується на розробленому методі знаходження точки простого порядку на повній ЕКФЕ, виконана задача пошуку загальносистемних параметрів криптостійких ЕКФЕ, які можуть бути рекомендовані для стандартизації. Отримано 40 повних кривих Едвардса над простими полями з модулями p_{192}, p_{224}, p_{256}, p_{384}. Розраховано порядок кривої $N_E = 4n$, якщо число n просте, можна порівняти за довжиною з довжиною відповідного поля (в межах 180 - 600 біт). Така крива може бути рекомендована до застосування в асиметричних криптосистемах.

З застосуванням Алгоритму 3, який базується на розробленому методі знаходження точки простого порядку на скрученій ЕКФЕ, Знайдено загальносистемні параметри криптостійкі 25-ти скручених ЕКФЕ над простим полем у всьому діапазоні стандартних значень модуля поля, придатних для стандартизації (прості поля с модулями довжиною 192, 224, 256, 384 і 521 біт, які рекомендуються стандартом FIPS-186-2- 2000). Вперше знайдені скручені ЕКФЕ для модулів поля p_{521} з найвищим стандартним рівнем стійкості, які рекомендовано для застосування в асиметричних криптосистемах зокрема стандартах ЦП.

Перелік використаних джерел до розділу 4

1. Бессалов А.В., Телиженко А.Б. Криптосистемы на эллиптических кривых: Учеб. пособие. – К.: ІВЦ «Політехніка», 2004. – 224с

2. FIPS 186-2. Digital Signature Standard(DSS). National Institute of Standard and Technology. January, 2000.

3. Бессалов А.В., Дихтенко А.А. Криптостойкие кривые Эдвардса над простыми полями. Прикладная радиоэлектроника, 2013, Том 12, №2.– С. 285-291.

4. Бессалов А.В., Дихтенко А.А. Определение параметров криптостойких кривых Эдвардса над простыми полями. XVI международная научно-практическая конференция«Безопасность информации в информационно-телекоммуникационных системах». 21 – 24 мая 2013 г. Тезисы докладов. – К.: ООО «ИП Эдельвейс», НИЦ «Тезис» НТУУ «КПИ», 2013. – С.36-37.

5. Бессалов А.В., Олешко К.А., Поречная Д.Н., Цыганкова О.В., Черный О.Н. Криптостойкие скрученные кривые Эдвардса с минимальной сложностью групповых операций. Прикладная радиоэлектроника: научно-техн. журнал. – 2016. – Том 15. – №3. – С.141 – 150.

6. Бессалов А.В., Діхтенко А.А. Кривые Эдвардса над простыми полями с почти простым значением порядка. Матеріали Двадцятої всеукраїнської науково-практичної конференції "Інноваційний потенціал української науки -- XXI сторіччя". Квітень, 2013.

7. Bernstein D.J., Lange T. Faster Addition and Doublingon EllipticCurves // Advancesin Cryptology—ASIACRYPT’2007 (Proc. 13th Int. Conf. OntheTheoryandApplicationofCryptologyandInformationSecurity. Kuching, Malaysia. December 2–6, 2007). Lect. NotesComp. Sci. V. 4833. Berlin: Springer, 2007. PP. 29–50.

8. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Теорія, практика, застосування: монографія. – Харків: Видавництво «Форт», 2012. – 870с.

9. Moloney R., McGuire G. Two kinds of division polynomials for twisted Edwards curves.Applicable Algebrain Engineering, CommunicationandComputing, 2011, PP. 321-345.

10. Бессалов А.В. Эллиптические кривые в форме Эдвардса и криптография: монография/ А.В.Бессалов. – Киев: КПИ им. Игоря Сикорского, изд-во «Политехника», 2017. – 272с.

ВИСНОВКИ

У дисертаційній роботі розв’язано актуальну науково-практичну задачу, яка полягає у розробленні нових методів підвищення швидкодії асиметричних криптосистем з використанням властивостей криптостійких ЕКФЕ над простими полями, які дозволяють підвищити швидкість експоненціювання точки та швидкість знаходження генератора криптосистеми. Проведені дослідження дозволили отримати нові наукові результати, які мають переваги перед існуючими та перелічені нижче.

1. Аналіз існуючих досліджень показав, що при описанні властивостей ЕКФЕ виникають суперечності щодо їх належності до певних класів, через некоректність існуючої класифікації. Із застосуванням методу перебору властивостей параметрів кривої існуючу класифікацію ЕКФЕ було удосконалено, що надало можливість описати властивості та умови існування трьох класів ЕКФЕ, що не перетинаються: повних, скручених та квадратичних та визначити кількість ЕКФЕ з мінімальним кофактором порядку кривої $N_E = 4n$, (де n – просте число) які мають більш високу швидкість експоненціювання точки, завдяки чому їх доцільно рекомендувати до використання для розроблення методів підвищення швидкодії алгоритмів криптосистеми.

2. Розроблено новий метод зниження складності виконання операцій додавання та подвоєння точок ЕКФЕ, який базується на виборі мінімальних параметрів кривої, що надає можливість зменшити складність додавання та прискорити швидкість експоненціювання точки.

3. Вперше проведено порівняльний аналіз швидкості експоненціювання точки кривих у формі Вейєрштрасса та ЕКФЕ методом розрахунку кількості операцій при скалярному добутку точок кривої за результатами якого було визначено, що найменших обчислювальних витрат вимагають операції на ЕКФЕ, особливо при подвоєнні, яке обходиться без операції множення на параметр

кривої, завдяки чому імплементація алгоритмів на ЕКФЕ швидше ніж на кривих у формі Вейєрштрасса більш ніж у 1,5 рази.

4. Розроблено нові методи знаходження точки простого порядку на ЕКФЕ над простими полями, розроблені на основі методу знаходження максимального порядку випадкових точок ЕКФЕ, які, за результатами порівняльного аналізу, швидші від існуючих стандартних методів у O(log$n$) разів (де n – порядок генератора). Проведені дослідження дозволили запропонувати три нових методи знаходження точок простого порядку для побудови алгоритмів пошуку генератора криптосистеми на повних та скручених ЕКФЕ, які швидше стандартного алгоритму ЦП на кривих у формі Вейєрштрасса у 180, $16\log(n)$ та $32\log(n)$ (де $n \in \mathbb{P}$) разів відповідно.

5. Розроблено три нових алгоритми пошуку генератора криптосистеми на підставі розроблених методів знаходження точки простого порядку та методу зниження складності виконання операцій, з використанням яких розраховано загальносистемні параметри 25 криптостійких скручених ЕКФЕ з урахуванням сучасних вимог щодо стійкості асиметричних криптосистем в рекомендованих стандартами FIPS-186-2-2000, FIPS–186–4-2013 та ISO/IECCD 15946 простих полях з довжиною модуля 192, 224, 256, 384 і 521 біт, які можуть бути рекомендовані для використання в асиметричних криптоалгоритмах.

6. Отримані результати були впроваджені та використовуються у Службі зовнішньої розвідки України, а також в навчальному процесі кафедри математичних методів захисту інформації Фізико-технічного інституту КПІ ім. Ігоря Сікорського при викладанні дисципліни «Криптосистеми на еліптичних кривих».

ДОДАТОК А.1

Параметри криптостійких повних кривих в формі Едвардса майже простого порядку $N_E = 4n$ (n – просте) над полями с модулями довжиною 192, 224, 256, 384 и 521 біт:

Таблиця 1 - Повні криві Едвардса майже простого порядку над полем з модулем p_{192}

$p =$	**FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFFFFFFFFFFFFF**
$d =$	28453E
$n =$	4000000000000000000000001AEAD1229D137F564D7FF6D5
$x_G =$	AE709D07B2D112CECD4A7AE103757F2C101D054ACB1A0F17
$y_G =$	8BDF8D5A994AAB1E1455889D28E29CA3EC68548D3F7CA32F
$d =$	6DBA6A
$n =$	3FFFFFFFFFFFFFFFFFFFFFFEA75D4027230DD4DFFDB0455
$x_G =$	44F083BB00E51AD91A2743284D31F57EE5C84826FCC91F4B
$y_G =$	15FC16E5870524E0DBBE9EC8BB9F066C02A02B1978D4E029
$d =$	CE37DC
$n =$	400000000000000000000000002618428A483A133570834389
$x_G =$	508AEB91AB9A230C377BD82BDDBE5B75CD38CDF1DA407A3C
$y_G =$	6E12D78C595D0ECC1614BFD04616CE45D6BB7D8607BB2ED7
$d =$	111DB4A
$n =$	400000000000000000000000004F2EA0DD45656E7E6066E8C9
$x_G =$	1603A0943674DA7D8476608E764BA7A63DBEBE4D8E549165
$y_G =$	148D5DA4654152C9196699074374EE091FE789A0CC7EC60
$d =$	12CCB98
$n =$	400000000000000000000000006AF187D9A93890273705F7E9
$x_G =$	6AC4FE0FEF645CA5754BFB0BD05967A418FCCAAF20E473A9
$y_G =$	B2F122E8816B142765B0FABCD7834CDC2D1AAC7EA779750B
$d =$	BFFAB4397C01049E12A46027E7E14D7A666240E6831D926
$n =$	400000000000000000000000022F2FB1AD838D6680571D7BB
$x_G =$	B46D3402D2A7F4CE30C5AA7839B0CE8D957240684824C726
$y_G =$	F0B24C20880DE704123ADF2A44189480DDFFDEEAF002B238
$d =$	CAE5B27FA36F62C6EC5EEC6ABE086C2BFF6A9F029CE42C88
$n =$	3FFFFFFFFFFFFFFFFFFFFFFFBD410EA5F77DD3ECCBD0FC45
$x_G =$	72F6A4BADEB19F876258926630ECA22F1D9FEF34CE53440C
$y_G =$	852D88019C7A20987BEE784A9EC09FF213639E59A3C3A51E
$d =$	2FDE6BF890C01A5FEB8B8D976676DDAC8C3349FE0C89959A
$n =$	3FFFFFFFFFFFFFFFFFFFFFFFC9B03E26E57C1A34245E23ED
$x_G =$	F2FA1F9E30FDF9C5CD1E84D287CE5F2DE9283B077C2C83FA
$y_G =$	419A50AF660CBF77699FBECBF7181F7F15C0DCF31523171F
$d =$	83E48CF4C49FDDEF6E5D812D3FBD06054835C85D6DD283BC
$n =$	400000000000000000000000002640829409C3B60282409D8B
$x_G =$	5BCFE7F1248E5A43CDF179D95334FE45061F0ECB599020B2
$y_G =$	FDEB479483DB5D1743AE7496B9A32B5CF774B8D8CD13272F

Продовження таблиці 1	
$d =$	CFC522DAB7BE9E92FA78DDA10CE941CC7108A299FB4A79C9
$n =$	4000000000000000000000006B362B3138DB79B9866A5BD7
$x_G =$	BE321DFF94A4E7DA940394E9C9EC1F2BC4B29F93302BDA3B
$y_G =$	B5E1CE7F685CEFE82284E5027404FE6E8D3C11E7D37092F3

Таблиця 2 - Повні криві Едвардса майже простого порядку над полем з модулем p_{224}

$\boldsymbol{p} =$	**FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF000000000000000000000001**
$d =$	3608425
$n =$	40000000000000000000000000020BBEC47CEDB34DD05BCB6B7E619
$x_G =$	C448CA02660F57204FF1BDE2B5CC3E25606A7460399FEA3DA9A06383
$y_G =$	319117770D6FC7FE35F6A02905FE1F363156BD2E5B75BB89A64CAFAB
$d =$	42E5CF5
$n =$	40000000000000000000000000070D1AD037FD1F2585B37C3CD8E75
$x_G =$	74E8DA9676A0AA64C73460EFBA56F04A5D69FB39DC03A0D53B9E99A9
$y_G =$	A70D758DE2B7CADCEED9D6315F44987AF89B9D1D3BB62B54574971D5
$d =$	148CD57
$n =$	40000000000000000000000000001BE5276AAC300270278233024CF9
$x_G =$	EEA0CBD1BFB937E1C83C12E90200429DD3F74854256DA5E249B04A2B
$y_G =$	512F075B98B7281E07BDABF68CE2BF4A30200DB1A9029ABDAAAEDEEA
$d =$	2C4C61C
$n =$	40000000000000000000000000054547A5F0105F649731ECC684CF
$x_G =$	142954F6B9702D136634AD2F6574ED5CF24E2D7D8AEB0B855105451A
$y_G =$	6EB430B9BE6B0A78D41BCBCFC3A207D0A813C8AB052BFD23529D23E9
$d =$	2DD96A9
$n =$	40000000000000000000000000024E3FE6372F8DB77945FFF06024D
$x_G =$	C62E8C8EB908FFC6DAE6D79D335618D62855B9A14F49DF1DEE0A414E
$y_G =$	6955A4D991CFE25E6EE21B64FC61763C16634CA234222A0E752F4E85
$d =$	1968A1D7A81AF44243D0F60F186A519FB95BF7C2FE2C037798D70FE9
$n =$	40000000000000000000000000003FCA1753F6F54C2A869DC8C5DBD9
$x_G =$	6F39E721F18128534C6C0339A982011683D9676565CAFD942F8C7761
$y_G =$	2E5ECC135081FE6FF9E0F7020BBC7EFD9DFB18A47B81DB825FC26817
$d =$	60B4BE2A9399C390AA051FC8B4706856E1CE2A03791C1B5A2C88DD40
$n =$	3FFFFFFFFFFFFFFFFFFFFFFFFFFFF5722B78ED1CA9B003572246F325
$x_G =$	60D6B139288C1B171E8FE28EC068130CABDA0A1A48C1DF7280A14211
$y_G =$	198E5F9E549D6C080CCCA7886E6BC880623B5AB1070CB62A81377BC0
$d =$	E3850F8A3D93759F172493E9339B29DB7D345BE57CFCDCE545EEB1DC
$n =$	40000000000000000000000000005B3B3E37B9EDE0A1B45BEC627F5B
$x_G =$	DB921A45CBF9979A3425F0556165DEF73ED6792034A9D9A5DC180FC9
$y_G =$	A3A87DA7A0307AD196B2CEC840C3E17147C570EBE9CC432DBF941CD7
$d =$	6E6607C2DCE3392468455ED0DBFBA5442AD87C7B8CE484C1B85D592
$n =$	3FFFFFFFFFFFFFFFFFFFFFFFFFFFFE623254CA68DF10B09B50D57327B
$x_G =$	96C7C00D85C8BB5B53F74E6EF38EFEEB458FE9434290046114E0E906
$y_G =$	A2410947B7C669193EC0B39001FC786B0558C3DBB6B64BC9677A7016
$d =$	2BFE721565BE78DE5DABD588BCE5E62C7127A0BEC33A2FF844E0B79D
$n =$	3FFFFFFFFFFFFFFFFFFFFFFFFFFFCCA2B4C227A60815F6A6359225E9
$x_G =$	DA2B86A81DBF8B887D3A3552A26CF3679DC73C300998BD82EEC1F49C
$y_G =$	D817BCDA64B37A31B2A15975F472A18F8D226446D1473CB3FB38D7C

Таблиця 3 - Повні криві Едвардса майже простого порядку над полем з модулем p_{256}

$\boldsymbol{p} =$	**FFFFFFFF00000001000000000000000000000000FFFFFFFFFFFFFFFFFFFFFFFF**
$d =$	72A38
$n =$	3FFFFFFFC00000003FFFFFFFFFFFFFFFBA76FA29C30CC3AA4954B53EDBE54D75
$x_G =$	894F8283626AEE6848515DDDC3B8DBB3D5302DEE0EE75080D6753E4D39BA5AB2
$y_G =$	EA612346223F6480CBBAFA39DB95D54D21469DD3074A957EFDA4FD79FEB630B5
$d =$	2EBFA9
$n =$	3FFFFFFFC0000000400000000000000005EFF905BA96F95CE79513CBE0CC53D1F
$x_G =$	363D655BF3F221256F032FC791B06149C14ACFFD92B59C84D1D3B817A9E622D2
$y_G =$	A52438C53DDCA661685B1F235EF0F1D280A493C33153AD691097AEC67A62C564
$d =$	805294
$n =$	3FFFFFFFC000000040000000000000051814C8E8360B7C96A8419F38B8039F1
$x_G =$	EEBABE42482F67FECF7F9D2D49A4430372D7678CF7EDAB4B9184D42BD93F390C
$y_G =$	E2A059E8C776F46028BA9265E20C09A785ECEEFB162562DA2AF78BC412D2D3CC
$d =$	9855C9
$n =$	3FFFFFFFC000000040000000000000002C1564946E895DAE0EB7EB501C62C62F
$x_G =$	D139CE35F84CFA17E8ED28E083F07C708303AE788477118C5AFE86D313D443BD
$y_G =$	F5F4A5309EEA75820AEE714A8D99CD22CE2539E73D2C6688B8480E18F1D384D
$d =$	BE957B
$n =$	3FFFFFFFC000000040000000000000005DACD9D621DE8444CB5625A8193E1D81
$x_G =$	B1550150B88C76AEC1CD0B0EC2008D1D73D086A0FD63103A0875EF574F0FF113
$y_G =$	306021DA97347B1DA05C98CE858B5C69ED901187DB03F68C399B694003FACA96
$d =$	4A5084ABF5DFFAC393E29A8BF045F4AA94C80F55414AFDAB8517CE769130DC82
$n =$	3FFFFFFFC00000003FFFFFFFFFFFFFFF9B91248CDD0CAF813BD0F8B9F32C892B
$x_G =$	96540A02F26ED385B606A7956E5BA33B8D5A9E47FCE718C752562E2F2A6891E2
$y_G =$	ACDE96C64793B77B72DC71EB12508AAC629C4CCAA281BF164B73030EF382D9DE
$d =$	340B9C82867CD106FA7E1B11E9415A1099BB48C9A28F3B21A77E70C20E528839
$n =$	3FFFFFFFC00000003FFFFFFFFFFFFFFFFBE08C2E4E3DDB90FBAB306B69633071
$x_G =$	490659C09655C82EECDC109AC5F29E85DC94882E30916E9F21273AFE9D1B01AC
$y_G =$	9BB0A4609F48A8029AD9014BE7184E36A120B5789799DE52F4E7D8D90386F786
$d =$	32BBA52848792541A79779B4CFFF035903D2112814334C1BE3556A670A9D73D1
$n =$	3FFFFFFFC00000003FFFFFFFFFFFFFFFC0285F94E407693E8624559A0D329309
$x_G =$	9D39DB8088196DE49C37D787D64EEB9ECA6A762BE77D0FCBD0430DCCBB057C2E
$y_G =$	62ABD075DA7C26034514079E7B5000D4493BC4318C5A3E3856FAAB8724C5C0F5
$d =$	8884FA14412BC9B62B0C467262DA6BD8F529C01AAD09545B2A294D479B254B2F
$n =$	3FFFFFFFC00000003FFFFFFFFFFFFFFFC7D37AFE15BFD6994B8E6427BA368D27
$x_G =$	D5D245310DD89B88DFF59C2CAEC8DBE62000E53D0BB4051247B97DDF420158C
$y_G =$	444B435A604729B76A17E8F4B93A47DC62D7777C1B056DB727675D627CF749F1
$d =$	E49478138FFE7946F81C3AC55BBBE4D41B4DF660A3B118B007567650642 5D9FA
$n =$	3FFFFFFFC000000040000000000000300FC8D622E987518514DFF16654AAFB
$x_G =$	92967B57C8CAB56FBDE3C3B0568C336BE2FBBB875F3983281D38B173C80971B9
$y_G =$	F3270D7C8A827B913A0B10079555D7D2E3A1C64578A49A77A9C1E6B45C186E90

Таблиця 4 - Повні криві Едвардса майже простого порядку над полем з модулем p_{384}

$\boldsymbol{p} =$	**FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFEFFFFFFFF0000000000000000FFFFFFFF**
$d =$	12593A
$n =$	40000000000000000000000000000000000000000000005063576B5A9A0C3A2 3E9510EA680650B4884E63A2968DD71
$x_G =$	1FC0E8E61F599813E376D11F7510D77F177C2F1CDE19FD14D63A2EC5EAD4 D0DED1BD06676CCF365243BF3C0675A31B62
$y_G =$	F52B4FA352B257D7A102FA45C56A50CCBDB3DEC053D5610EDBD0188C11F 321F28A43E2FC50395E4A8BD0029AE71D51AA
$d =$	46959A
$n =$	40000000000000000000000000000000000000000000000C06E6B5CE557E3DD EC6844B3470B819A9E1C0ED5F348517
$x_G =$	4567EA938DECB2BC17F9ABDEDBD77AD188FEFD6E244FD8A12C95A365F9 C241E13888506D9D1FB4F8F9B8AA49098C3DF0
$y_G =$	121D587D9CEDEB34DD331E150D9FB2A23B314A354411C4F4A5AFF18685F6 EDA1D557EC99F830785420A4DAD15897814E
$d =$	5FD247
$n =$	40000000000000000000000000000000000000000000000A6A021C752BB1572 44080A30D578824A05A3BFFF4E67575
$x_G =$	8947F1251392317F3C0E127F7D337B1EE67A120BC69B5E1D91B6C7DC004904 C1D42013DE9F12176B6EB34AD5CAC2D485
$y_G =$	B934A355EC5F900123E5EFFDB74502E084A94E59BFDF80E2B0979D02F971F 0FE93A4ECE5FFC82C34724A2063836DA847
$d =$	7B35A8
$n =$	3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF96861B6F4CC0 29EE5B29F5BE0649FA4B3A605D3EC2CFD8F
$x_G =$	712160E70ED57AEC69A66E55A3A285DBFA712F9ACF9B334AC881E5066E55 A415BE5935881C7DF7AF90EF6558C380037
$y_G =$	F1FF700AB04A2CA0F40FD94F1E32F61A3D4638570A28EB07AD1D281DAAC 0293B946205098F71AC9BEBC8616F1B1DD3E8
$d =$	9302CE
$n =$	40000000000000000000000000000000000000000000000422338834D697FC314 9FC70C79239975452EA01F75E2B699
$x_G =$	E9FDD336AC467447D6DB0627563C181663797C6D87F8E66A3E61BE69E53F6 6CCC4847DF28A19235D9377F4A33FEE0F69
$y_G =$	CF9AC7F9EEB6528DF53C80BF02E3A83D07614F2708148B4F7F1907398DE79 019256D32E535219D71F173DEAE9621716B
$d =$	4CCEDF781B3680122FCFC696374F2ACA57E8F7514293BDD81F5040F0858023 ECD295E6835FC14021B1AFFAF8065139C9
$n =$	40000000000000000000000000000000000000000000000046824B5EE5BADD70E B246617456AD087BADECDA7CD2A6E81
$x_G =$	36AFEDFF2308CF4C2F2052B0BF3068F0B4EE9759729A40491EF5D5E75F23E7 4A6F8528D276E6C528F487DE35E71454CB
$y_G =$	94D6B53F630A6D41E4DD65CD195839CC24DE7B6A71C3DC0A814E379445C 67C6604B8034F7C5580AC0FBE771FBA1E9E36

Продовження таблиці 4

$d =$	3462B5F8DD2744C13ED8618BAFC853F60F83134B936F3DD2867562D1CEEA866E590D702CE8C11262193F077A798918DE
$n =$	400000000000000000000000000000000000000000000000339419162A90FA9A9CA9C0C12B231CF5D95CC5E241D18C0F
$x_G =$	387CCD92DDCF7203D579EC6D158AD3A4DBAB83BBA4E153FB130F380425FD9F73AABEE0F2BE3BCA53D9E1D798DB016F3C
$y_G =$	50E827613BC65DEC52FD123387279D4E9E27102CE6B9119DC656632ED043D3961C72EB7C67D690D970CC65DD2F7C5702
$d =$	941F6CCE649868BD59F335D3293FBB201E3C811ADE19779EEFD8FB21AC1A466377365A8763793A3B3BB2B6575D9893D1
$n =$	4000000000000000000000000000000000000000000000002E0E36DDDDC5D4EA80D339D03926CA39AE3A4739EF81A1C9
$x_G =$	647D270CE4CB1F9038EEE75ED9570A3360AC68DE443BE52D23A734966F813D690615BE4284BDD78CF89B4ED2D02BE08A
$y_G =$	32247232CFA0A712AE3B029B1DDF8C5FE86A78E5728CB4D4386026C21A92297C271C81294C7B9DC18E245F6D87706865
$d =$	584D94FEA391957947760106F180D57CFE8E85109656E4B0BF6FCBF69D62F9A649AEF53CDA9B9F3B2BB247DEB6AB0C70
$n =$	3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF8C7F4A394F5C92E8C6FB2FD97B1657DF603DB9677EEE6DD9
$x_G =$	4CAFBA0D62C538B7CC74F8274978AF35C43E2360BA6606FD379086367898EFD57040629FD9AC9721D65BCB511603BA00
$y_G =$	E2C024B79576CC47776562F9203B166E1C8300AD5C7F4D0B04FE0DBAF92FEC3DD0E5CE1F93288308D2C5CFF5B24DEC9A

ДОДАТОК А.2

Параметри криптостійких скручених кривих в формі Едвардса над простими полями з модулями довжиною 192, 224, 256, 384 і 521 біт.

Таблиця 5 - Скручені криві Едвардса майже простого порядку над полем з модулем p_{192}

$p = 2^{191} + 2^{16} + 2^{12} + 1$ p = 8000000000000000000000000000000000000000000011001 n = 2000000000000000000000004447D62B952200D604D2BEB9 a = 3 d = DD x_G = 79FD21DC7BF961D56CDD092798C3016F11C2034F154A94B5 y_G = 17B25C0DADFD379FF3D7CD1EAEFD83328B945410BE11D5DB
$p = 2^{191} + 2^{45} + 2^{41} + 1$ p = 8000000000000000000000000000000000000220000000001 n = 1FFFFFFFFFFFFFFFFFFFFFFFEAA490B04DCC3760DB69D80B a = 5 d = B7 x_G = 41D4C37EE995324B600442F0DCE31A0EA61C08C92D80110B y_G = 3EC06FDFB33AFA858E30D898F9C18606CA62E79F6175FD80
$p = 2^{191} + 2^{46} + 2^{36} + 1$ p= 8000000000000000000000000000000000000401000000001 n = 1FFFFFFFFFFFFFFFFFFFFFFFC219C1BBD9EF98692F7D3077 a = 3 d = 4D x_G = 50707DB9B16BF11C894E2A2F25A2887A6AB3A5921E9AACDE y_G = 1BEF37EF93DBA0D7203F96BD14FCDA0E6B1CF118866982B2
$p = 2^{191} + 2^{49} + 2^{27} + 1$ p = 8000000000000000000000000000000002000008000001 n = 1FFFFFFFFFFFFFFFFFFFFFFFD4622687DA3DDCBF47806983 a = D d = AC x_G = 3BFDC9D07301A8A3A9BEC18540B0EEDC0F7C3CD21F652EFE y_G = 3C48E70B7F04C446A8CC208696DA2592A56FB29C79888D52
$p = 2^{191} + 2^{158} + 1$ p = 8000000040000000000000000000000000000000000000001 n = 2000000010000000000000004DE2B37DC449E40E33C414B9 a = 5 d = 800000003FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFC0F x_G = 209295DA12CEDAE57617AF4911C57DDCE7043EB18687E13C y_G = 3847775699DF8A7F431D8DA8FE993A28A6D4F108B6502917

Таблиця 6 - Скручені криві Едвардса майже простого порядку над полем з модулем p_{224}

p= 2^{223} + 2^{24}+ 2^{20}+ 1 p = 8000000000000000000000000000000000000000000000000001100001 n = 20000000000000000000000003F330C2860F36EC9E831F641A2B9 a = 3 d = 93 x_G = 6C7CC9C10F4259CBEB0D1973AF0E4FC64AE442A301A90DFEEB5BC081 y_G = 2D4F15BA1A686CAEDB9D43F9525BF78683DAA39B82301FCA8A7874BE
p = 2^{223}+ 2^{38}+ 2^{36}+ 1 p = 8000000000000000000000000000000000000000005000000001 n = 1FFFFFFFFFFFFFFFFFFFFFFFFFFBCE784913191A6362578E1CD28C9 a = 3 d = 215 x_G = 60536D73F2A4EF1F54C1048734301E01306FF7F331719201335D5A55 y_G = DDBFD9D1AFD09CD322F639F524CC60F9A7A727139F56BBF8D127940
p = 2^{223}+ 2^{61} + 2^{41}+ 1 p = 8000000000000000000000000000000002000020000000001 n = 20000000000000000000000002165B89B7402F30BF010CB396EA9 a = 5 d = 3D x_G = 59507C9FEF622459507C9FEF622459507C9FEF623AAD7109DDBA6AF7 y_G = 1366A5B9781878270245AAA111E53CDC079B0322CB4A8C805309452A
p = 2^{223}+ 2^{72}+ 2^{20}+ 1 p = 8000000000000000000000000000000010000000000000100001 n = 1FFFFFFFFFFFFFFFFFFFFFFFFFFE0DAC7710567C631D4CA120783E9 a = 3 d = 15C x_G = 5C611714E8FD05D966F07BD978DF524642C21CF3BDBB6BA1FE037DD8 y_G = 3499A41BF2C767BD41A045CDB7285F9E4907598421C0B78D29D5A7E0
p = 2^{223}+ 2^{66}+ 2^{14}+ 1 p = 8000000000000000000000000000000004000000000004001 n = 20000000000000000000000000014E4DE701954CB43404E060EAC01 a = 3 d = 26 x_G = 2A795ABA13A5D9DC2BEB32468049F7E8E287393711EA0A66DCBFF040 y_G = 532C172BF052220CDE0B63A2F421DB65E8A676B96D7FA0307DDC0E53

Таблиця 7 - Скручені криві Едвардса майже простого порядку над полем з модулем p_{256}

$p = 2^{255} + 2^{46} + 2^{42} + 1$ p = 8000000000000000000000000000000000000000000000000440000000001 n = 2000000000000000000000000000330A60EA43DF5957AC18C44AB8122EB7 a = 3 d = 1AF x_G = 25091FBF427205B62204FD7FE48236752C1FE497EF2DB3197938BA36D9A27554 y_G = 52A7749533218F16BB1F32137CE731DC0F26149CE2E1CF1378B74E066B952532
$p = 2^{255} + 2^{41} + 1$ p = 8000000000000000000000000000000000000000000000020000000001 n = 2000000000000000000000000002498CDC14EB2676199F9EFB8C86EA9D1 a = 3 d = BC x_G = 1306A0056F9B6F44758D8146286E140B8D2A4C7179CCB2B515E9EAE4A679F81 y_G = 33CD1A3853C6059B39DE2485F320CC00D97E1BB77D5C79025BF01D1F3C0D8868
$p = 2^{255} + 2^{66} + 2^{60} + 1$ p = 8000000000000000000000000000000000000000041000000000000001 n = 200000000000000000000000000002BC056BB954BD3CF60CD27D370FF3265 a = 3 d = 6C x_G = 7E5D3187BA7FF18EF3066E57C722DCE95279A01945D6B4C2E918B56C32FF35D1 y_G = 3AC8B7A5A64DA05FF1F28870506E451F103DA6EE32FAB89D3D903E073660572E
$p = 2^{255} + 2^{38} + 2^{2} + 1$ p = 8000000000000000000000000000000000000000000000004000000005 n = 200000000000000000000000000031F23720CCCC83EF9F44858B6E952E4F a = 2 d = 1CC x_G = 25091FBF427205B62204FD7FE48236752C1FE497EF2DB3197938BA36D9A27554 y_G = 52A7749533218F16BB1F32137CE731DC0F26149CE2E1CF1378B74E066B95253
$p = 2^{255} + 2^{70} + 2^{66} + 1$ p = 8000000000000000000000000000000000000000044000000000000001 n = 200000000000000000000000000002B81184994F3F0880BB2B78314AFD2E9 a = 3 d = 13A x_G = 1C32148FB9F80F78D2E84879553296DA0858C29EFEAD3EDCCBFC55E8FEE15C85 y_G = 2D4ED6C59052B9113E76AEDACBC668F3BB0EE5819C5B5221A311118DECAAE65E

Таблиця 8 - Скручені криві Едвардса майже простого порядку над полем з модулем p_{384}

p = 2^{383}+ 2^{155}+ 1 p = 800000000000000000000000000000000000000000000000000000000000000080000000000000000000000000000000000000000000000001 n = 1FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFE935B9B743CFBDC890CDB6FC507DB7744384DF7B5FAF81D1 a = 3 d = EC x_G= 5B83FE601E531F45B83FE601E531F45B83FE601E531F45B83FE601E537AC9B6A004550477AC9B6A004550477AC9B6A004550477AC9B69FF y_G= 5FF608B37764C7FE1719D75DA24646D8869E60637F0C477A548C46BDECB0270BF2C840E083654F63367D737325053472
n = 1FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFD2E846F4DD24CB4DC3014E1B9B39C56950B3F5FF1870523 a = 3 d = 10A x_G= 2301C9793214FC6152B4CEED1379498ACA6F87089186C2301C97932151F631C2E01020FDA9C3F995C9A81DB118C9FA39 y_G = 79AFEE927FA08107917851B6F7DD952DC852C052D6A2DDE0E0E1AF9EA781CDC8AF1ED4E9B024BFA5FAB992443F80C745
p = 2^{383}+ 2^{233}+ 1 p= 800000000000000000000000000000000000020000000000000000000000000000000000000000000000001 n = 2000000000000000000000000000000000007FFFFFFFFFCEA783C2F07E63118A47FDB07FBAD3E742437E35EA11EA81 a = 3 d = 15A x_G = 45FB6177745030C78D712C115E5354E6F6AB496E668C3DB6A55EB1EF2F9418052C6FF89BF253B3813F48B5134EFD5220 y_G = 35525C097B1F9D1DB5ABB1695B62EF88E79DDCE007ACD8F167E7022A2EC379AF0A7C184F8C09934F230A30522FA27EE3
n = 2000000000000000000000000000000000007FFFFFFFFFC4E3F96E2B485B72DB4DC623D7ECECFE59A562991D60A279 a = 3 d = 7B0

Продовження Таблиці 8

x_G = 5EE2C5033D54291ACD632030F57D0AD23E537766CAEF2EC8E7117FA4D247D71E488F0F AA45B5A1E8FEA7E6617BFA140E y_G = 39949C9783884C7491E5D3F0D33704A278A6D4DF52C56C9B83FDC59BCF9282A42BFB06 B377CF4E00933842AD9B65511
n = 20000000000000000000000000000000000000007FFFFFFFFFFB43327D7C94B4BEA93CCCFC A103CF64D6A40B8F00E9016B a = 3 d = 33B x_G = 56499011F2275F6A3E9421923C69AA0F8C47A25BD16EF68635243D6B1867A732DC11CA8 C8CEFF30132EFDF33C9B2B969 y_G = 46D521F9D3A98FF01C4D5676A6CBB88A78AB84F2502A0A30E9A51A64A26D60FD47F8B 02E0B5F1713783CFC878DAF6108

Таблиця 9 - Скручені криві Едвардса майже простого порядку над полем з модулем p_{521}

$p = 2^{520} + 2^{66} + 2^{65} + 1$ p = 100000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000060000000000000001 n = 40000000000000000000000000000000000000000000000000000000000000001E5EE0522024 E5E359E578FDD4AAE5B3388CCE2795EC03189792778B80EDB1251 a = 3 d = 2A8 x_G = BA5B99F7375F86F6D700E0DCD8E750E64FE9EA4F44B5C4CF022B45EDD2B81962129B6 AED970FCAF0754EA418054E5AAB55FD9911C 3BBAA99DB75F86F6D700E0DCD y_G = 91E0646D69810E9FC606F87EA7BFA7140B1446EEA937536CDDC166C301BB0ECE279DA 15838913154E7BEDE69C7AC43D2756A279005 625F52F9D145A41E77E31D4B

Продовження Таблиці 9

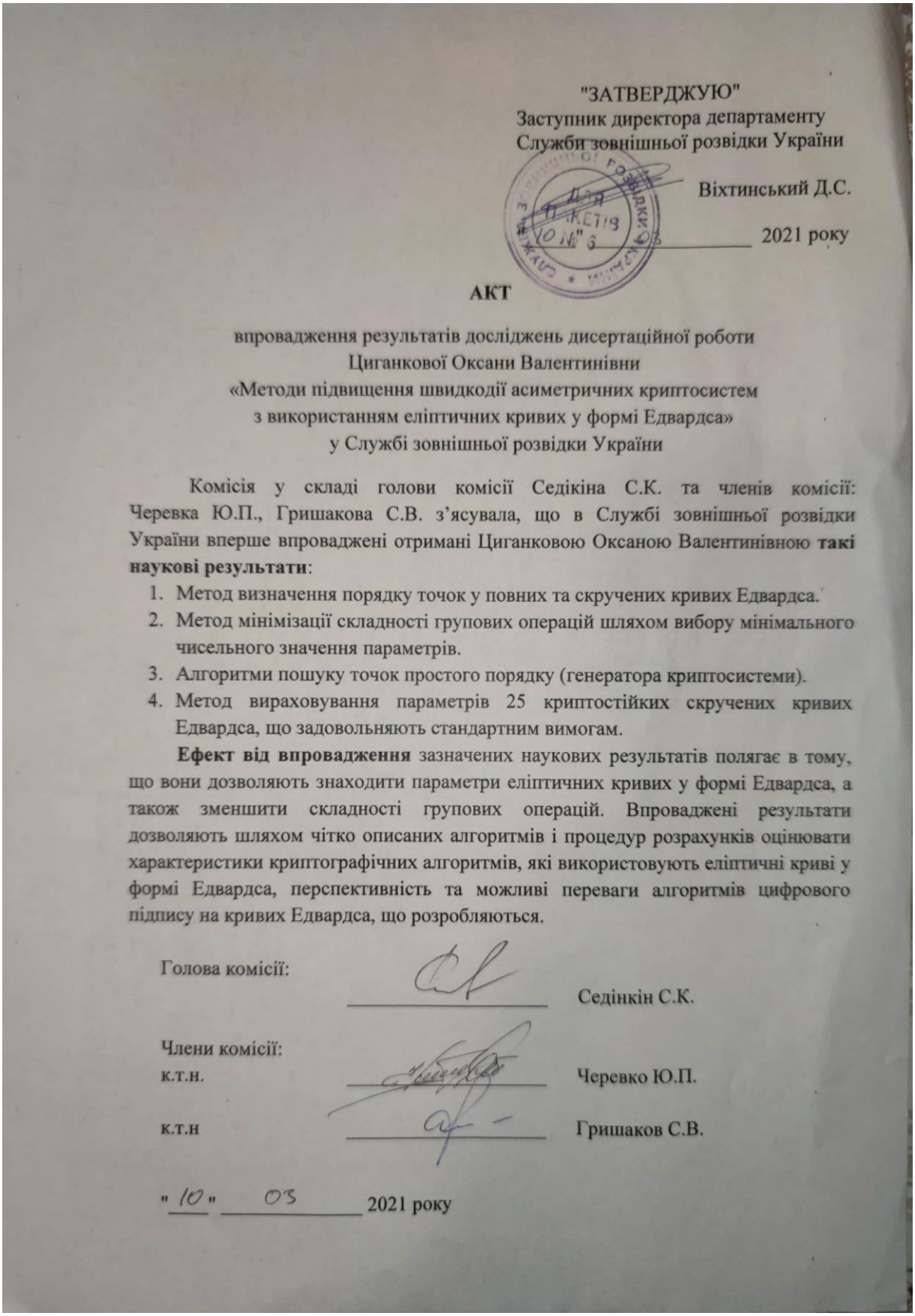
$p = 2^{520} + 2^{80} + 2^{39} + 1$ p = 100000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000100000000008000000001 n = 3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFD4F3 EBC074E5DCC909AAE45C02D90E60764C007 6526D0C9B9F66517F45515A05 a = 3 d = 87 x_G = 6287A808BC52FD146441B870582B459B154149EC3E444F88F3950A07DF4AC946781D7517 D86287A808BC52FD146441B870582B459B154
1AC73E64D0C0D347D72A7 y_G = 6A20EC64258785F16B2A400BF0C6D2E90C8080AE25A96F465029EE2A148A0EF2BF0DF9 E087F1E02487738C927BAF4B0C50A9349BA68 FAF1D3B24BB6E0D8E991B1
$p = 2^{520} + 2^{110} + 2^{4} + 1$ p = 100000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000004000000000000000000000000011 n = 3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFBE822 ED9ECC69628BD3C3257DB51B5FC7477094B E7A8266F720BFB22D9AA02123 a = 5 d = D2 x_G = DE935EF49AF7A4D7BD26BDE935EF49AF7A4D7BD26BDE935EF49AF7A4D7BD26BDE93 5EF49AF7A4D7BD26BDE935EF49AF7A4D7B
D5E62C0F3160798B03CC581E62C1C y_G = 7CD02BB98782E14860C91A53E907B7C4FDAA1C6898375790CB3FDED238FD9A069B8C5 3B67AC5DC0C8B782D74624A69D91450D20C C9DCA8B76DB97994008CB492F1

Продовження Таблиці 9

$p = 2^{520} + 2^{348} + 2^{278} + 1$ p = 100000000000000000000000000000000000000000010000000000000000040000000000000000 00000000000000000000000000000000000000000000000000001 n = 4000000000000000000000000000000000000000000400000000000000000FFFFDCB98F10F9C F70F01865640CBDD9D354DDFB78BBD8EE3F20DD416BE23E0E1D08D a = 5 d = 53 x_G = D8F7F6D0EEC7BFB687763DFDB43BB1EFEDA1DD8F7F7A9E6BE90A54F35F4888E598AE 7E472CC573F239662B9F91CB315CFC8E598AE7E472CC573F239662B9F91CB2 y_G = FDB9481BBAFC22AD99D0C546F5B6C6809013308A794235AEE551A74142CBE4695FD237 08A6C27631A6AF3DF61BB4F83C481614132F713D0B860EAB37B7F74748D2
$p = 2^{520} + 2^{73} + 1$ p = 100000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000002000000000000000001 n = 3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFD34B6 3B11FF960C064B6AEA3B6851C23CCDC50B6E6921941026DF9E4883D1C157 a = 7 d = 100000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000001FFFFFFFFFFFFFE786B x_G = 4CFD4C477A7FABB556313753CD284B6B2315E866A9C3A38F399E19FCEC6BA0796367A FBD7B6AAE33967252EA110AF880CB1038A2E699072C8FACACCF0F919B3C67 y_G = 74E83FF02F90FB98F028FC1D0BD94A0093E94E6250BA9DDEE68F1DE65242E496D90B9C EAE817717DFB7EC4E9E2D7A0004FDBB99B2 79AA75BF2E785DB9A5D415EBA

ДОДАТОК Б

Акти використання результатів досліджень дисертаційної роботи



"ЗАТВЕРДЖУЮ"
Заступник директора департаменту
Служби зовнішньої розвідки України

Віхтинський Д.С.

"10" 03 2021 року

АКТ

впровадження результатів досліджень дисертаційної роботи
Циганкової Оксани Валентинівни
«Методи підвищення швидкодії асиметричних криптосистем
з використанням еліптичних кривих у формі Едвардса»
у Службі зовнішньої розвідки України

Комісія у складі голови комісії Седікіна С.К. та членів комісії: Черевка Ю.П., Гришакова С.В. з'ясувала, що в Службі зовнішньої розвідки України вперше впроваджені отримані Циганковою Оксаною Валентинівною **такі наукові результати**:

1. Метод визначення порядку точок у повних та скручених кривих Едвардса.
2. Метод мінімізації складності групових операцій шляхом вибору мінімального чисельного значення параметрів.
3. Алгоритми пошуку точок простого порядку (генератора криптосистеми).
4. Метод вираховування параметрів 25 криптостійких скручених кривих Едвардса, що задовольняють стандартним вимогам.

Ефект від впровадження зазначених наукових результатів полягає в тому, що вони дозволяють знаходити параметри еліптичних кривих у формі Едвардса, а також зменшити складності групових операцій. Впроваджені результати дозволяють шляхом чітко описаних алгоритмів і процедур розрахунків оцінювати характеристики криптографічних алгоритмів, які використовують еліптичні криві у формі Едвардса, перспективність та можливі переваги алгоритмів цифрового підпису на кривих Едвардса, що розробляються.

Голова комісії: Седінкін С.К.

Члени комісії:
к.т.н. Черевко Ю.П.

к.т.н Гришаков С.В.

"10" 03 2021 року

«ЗАТВЕРДЖУЮ»

Директор
Фізико-технічного інституту
КПІ ім. Ігоря Сікорського
Олексій НОВІКОВ
«_9_» __лютого__ 2021 р.

АКТ

використання результатів досліджень дисертаційної роботи
Циганкової Оксани Валентинівни на тему
«Методи підвищення швидкодії асиметричних криптосистем з використанням еліптичних кривих у формі Едвардса»
на здобуття наукового ступеня кандидата технічних наук
за спеціальністю 05.13.21 – системи захисту інформації

Комісія у складі:
голови д. ф-м. н., член-кор. НАНУ Савчука М.М.
та членів комісії:
д. т. н., професор Ковальчук Л.В.
к. ф.-м. н. Завадської Л.О.

цим Актом засвідчує, що
результати досліджень дисертаційної роботи Циганкової Оксани Валентинівни на тему «Методи підвищення швидкодії асиметричних криптосистем з використанням еліптичних кривих у формі Едвардса» впроваджені в навчальний процес Фізико-технічного інституту КПІ ім. Ігоря Сікорського. Отримані Циганковою О.В. нові наукові результати використовуються при викладанні навчальної дисципліни «Криптосистеми на еліптичних кривих» магістрам Фізико-технічного інституту, яка відноситься до циклу професійних дисциплін другого (магістерського) рівня вищої освіти.

Голова комісії
д. ф-м. н., член-кор. НАНУ Михайло САВЧУК

Члени комісії:
д. т. н., професор Людмила КОВАЛЬЧУК

к. ф.-м. н. Людмила ЗАВАДСЬКА

«_8_» __лютого___2021 року

ДОДАТОК В

Апробація результатів дисертації

УДК 681.513.675
№ держреєстрації 0113U002468
КВНТД І.1 01.05.01
Інв. №

Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут"
(НТУУ "КПІ")
03056, м. Київ-56, пр. Перемоги, 37
тел. (044) 236 70 98

ЗАТВЕРДЖУЮ
Проректор з наукової роботи
академік НАН України
М. Ільченко
2015.12.15

ЗВІТ
ПРО НАУКОВО-ДОСЛІДНУ РОБОТУ

ЛОГІКО-ЙМОВІРНІСНИЙ ПІДХІД В ЗАДАЧАХ БЕЗПЕКИ СТРУКТУРНО-СКЛАДНИХ СИСТЕМ

д/б № 2602-ф
(заключний)

В.о. директора
Фізико-технічного
інституту
к.т.н., доцент
2015.12.03
Т.Литвинова

Керівник НДР
професоркафедри
інформаційної безпеки
Фізико-технічного
інституту
д. т. н., професор
2015.12.03
2016.12.05
О. Новіков

2015

Рукопис закінчено 17.11.2015 р.
Результати цієї роботи розглянуто Вченою Радою ФТІ протокол № 11/2015 від 18.11.2015р.

СПИСОК АВТОРІВ

Керівник НДР д.т.н., професор НТУУ «КПІ»	О. Новіков (Розділ 1, 2, 3, 5, 8, 10)
д.т.н., професор НТУУ «КПІ»	А. Качинський (Розділ 7)
д.т.н, професор НТУУ «КПІ»	А.Бессалов (Розділ 9)
к.ф.-м.н., доцент, с.н.с. НТУУ «КПІ»	С. Смирнов (Розділ 1, 4, 11)
к.ф.-м.н., доцент, с.н.с. НТУУ «КПІ»	А. Родіонов (Розділ 2, 3, 5, 8, 10,11, 12)
к.т.н., доцент, с.н.с. НТУУ «КПІ»	О.Куссуль (Розділ 6, 7)
к.т.н., доцент, с.н.с. НТУУ «КПІ»	М. Грайворонський (Розділ 1)
м.н.с., к.т.н., НТУУ «КПІ»	О. Барановський (Розділ 6, 7, 12)
м.н.с., НТУУ «КПІ»	М.Ільїн (Розділ 12)
м.н.с. НТУУ «КПІ»	А. Хнигічева (Розділ 2, 6, 7)
аспірант НТУУ «КПІ»	О. Циганкова (Розділ 9)
Організаційно-аналітичний відділ	З. Кравець
Нормоконтроль	Н. Рябцева

УДК 681.3.06:519.248.681
Держ. реєстр. № 0117U000500
код КВНТД І.1 01.01.08,
Інв.№_____

Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
(КПІ ім. Ігоря Сікорського)
03056, м. Київ-56, пр. Перемоги, 37 тел. (044) 236 70 98

ЗАТВЕРДЖУЮ
Проректор з наукової роботи
д.т.н., професор
_____ В.А. Пасічник
08 01 2020р.

ЗВІТ
ПРО НАУКОВО-ДОСЛІДНУ РОБОТУ

ДОСЛІДЖЕННЯ МЕТОДІВ КРИПТОГРАФІЧНОГО АНАЛІЗУ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ В КЛАСИЧНІЙ ТА КВАНТОВІЙ МОДЕЛЯХ ОБЧИСЛЕНЬ З УРАХУВАННЯМ ДОДАТКОВИХ ДАНИХ ТА УМОВ ФУНКЦІОНУВАННЯ

д/б № 2030-п
(остаточний)
Частина 1

Директор
Фізико-технічного
інституту док.тех.наук,
професор _____ О.М. Новіков

Керівник НДР
В.о. завідувача кафедри
математичних методів
захисту інформації,
член-кореспондент
НАНУ, д. ф.-м. н. _____ М.М.Савчук

2019

Рукопис закінчено _____ 2019 р.
Результати цієї роботи розглянуто Вченою Радою ФТІ протокол № 13/2019 від 25.11.2019р.

ДОДАТОК Г

Перелік публікацій за темою дисертації із зазначенням особистого внеску здобувача.

1. Бессалов А.В., Цыганкова О.В. Взаимосвязь семейств точек больших порядков кривой Эдвардса над простым полем. Bessalov, A.V., Tsygankova, O.V. «Interrelation of families of points of high order on the Edwards curve over a primefield» // English translation of Problems of Informati on Transmission, 2015, Vol. 51, № 4, pp. 391-397. Іноземне видання Scopus, WoS. *Здобувачу належіть модифікація закону складання точок на ЕКФЕ над простим полем.*
2. Бессалов А.В., Цыганкова О.В. Число кривых в обобщенной форме Эдвардса с минимальным четным кофактором порядка кривой. // Проблемы передачи информации. Москва – Том 53, Вып. 1, март 2017, С. 101-111. *Transmission:* Bessalov A.V., Tsygankova O.V. «Number of curves in the generalized Edwards form with minima leven cofactor of the curve order» // English translation of Problems of Information 2017. Іноземне видання Scopus, WoS. *Здобувачу належіть побудови методів знаходження точки простого порядку на ЕКФЕ.*
3. Бессалов А.В., Цыганкова О.В. Новые свойства эллиптической кривой в форме Эдвардса над простым полем. // Радиотехника №180, 2015. – С.137-143., Bessalov, A.V.,Tsygankova, O.V. «New properties of the Edwards form elliptic curveover a primefield» // Telecommunications and Radio Engineering (English translation of Elektrosvyaz and Radiotekhnika) 2015. (проіндексовано в міжнародних наукометрічних базах Scopus, Web of science). *Здобувачу належіть застосування подвійної симетрії координат точок для аналізу їх властивостей.*
4. Бессалов А.В., Цыганкова О.В. Производительность групповых операций на скрученной кривой Эдвардса над простым полем. // Радиотехника №181, 2015.– С.58-63. *Здобувачу належіть оцінка складності операції подвоєння точок на ЕКФЕ над простим полем.*

5. Бессалов А.В., Цыганкова О.В. Метод определения точек максимального порядка на кривой Эдвардса. //Спеціальні телекомунікаційні системи та захист інформації. Збірник наукових праць, випуск 2 (26), 2014. С.18-21. *Здобувачу належіть постанова завдання щодо пошуку: які властивості ЕКФЕ дозволяють знайти випадкову точку максимального порядку.*

6. Бессалов А.В., Цыганкова О.В. Классификация кривих в форме Эдвардса над простым полем. // Прикладная радиоэлектроника, 2015 Том 14 № 3, , С.197-203. *Здобувачу належіть систематизація ознак класифікації кривих в узагальненій формі Едвардса.*

7. Бессалов А. В., Третьяков Д. Б., Цыганкова О. В. Свойства точек малих порядков кривых в обобщенной форме Эдвардса // Сучасний захист інформації № 2, 2016, С.46-54. *Здобувачу належіть аналіз особливих точок 2-го порядку ЕКФЕ.*

8. Bessalov A., Dykyi V., Malyshko A., Tsygankova O., Yadukha D. Parameters of the Fastest Cryptographically Strong Twisted Edwards Curves . // Theoretical and Applied Cybersecurity 2019. 1. с.7-11. *Здобувачу належіть координація завдань виконавців розрахунків.*

9. Циганкова О.В. Нові алгоритми знаходження базової точки на еліптичних кривих у формі Едвадса // «Інформаційні технології та комп'ютерна інженерія» № 1 (47) 2020. –С. 39-47.

Тези конференцій

10. Бессалов А.В., Цыганкова О.В. Свойства точек больших порядков кривой Эдвардса // тезиси докладів XVII міжнародної науково-практичної конференції «Безпека інформації в інформаційно-телекомунікаційних системах», Київ. – К.: НДЦ «Тезис», 2015 р. – С. 30-31. *Здобувачу належіть порівняльний аналіз швидкодії розроблених алгоритмів знаходження генератора криптосистеми з чинними алгоритмами стандарту ЦП.*

11. Бессалов А.В., Цыганкова О.В. Классификация кривых в обобщенной форме Эдвардса. // тезиси докладів XVIII міжнародної науково-практичної конференції

«Безпека інформації в інформаційно-телекомунікаційних системах», Київ. – К.: НДЦ «Тезис», 2016 р. – С. 30-31. *Здобувачу належіть систематизація ознак класифікації кривих в узагальненій формі Едвардса.*

12. Бессалов А.В., Олешко К.А., Поречна Д.Н., Циганкова О.В., Чорний О.Н. «Криптостійкі скручені криві Едвардса з мінімальною складністю групових операцій» // тезиси докладів XIX міжнародної науково-практичної конференції «Безпека інформації в інформаційно-телекомунікаційних системах» Київ. – К.: НДЦ «Тезис», 2017 р. – С. 260. *Здобувачу належіть постановка задачі та участь у роботі групи дослідників щодо розрахунку загальносистемних параметрів 25 криптостійких скручених ЕКФЕ над простим скінченним полем.*

13. Цыганкова О.В., Цыганков Р.И. Анимация точек экспоненцирования кривой Эдвардса // тезиси докладів XV Всеукраїнської наукова-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики», 25-27 травня 2017р., м. Київ. Том II.– С. 114. *Здобувачу належіть графічна ілюстрація скалярного добутку точок експоненціювання ЕКФЕ.*

14. Бессалов А.В., Циганкова О.В. Умови існування суперсінгулярних повних кривих Едвардса над простим полем // тезиси докладів XX Ювілейної міжнародної науково-практичної конференції «Безпека інформації у інформаційно-телекомунікаційних системах», Київ. – К.: НДЦ «Тезис», 2018 р., – С. 119-120. *Здобувачу належіть участь в аналізі властивостей суперсінгулярних повних кривих Едвардса.*